California Child Support Automation System (CCSAS)
State Disbursement Unit (SDU)

INTERFACE TEST PLAN
CDL IM 008-1

Version 1.1

P-00004-1.1-042905

April 29, 2005

Prepared By:

California Child Support Service Provider (CCSSP)

LIST OF REVISIONS

Version No.	Date	Description
1.0	3/25/05	Initial Submission to State
1.1	4/29/05	Re-submission to address State's Deficiency Report

SIGNOFF

The Interface Test Plan has been reviewed and found in accordance with the requirements listed under Exhibit 6A of the Request for Proposal.

Name	Signature	Date

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 OVERVIEW

The California State Disbursement Unit (SDU) supports the centralized remittance and processing of child support collections and is located in Sacramento, California. The SDU Service Provider (SP) will perform the collections and disbursement processing of child support payments for the State of California.

1.2 PURPOSE

This document provides a plan for preparing, managing and evaluating the various tests necessary to ensure accurate processing of interface files. Specifically, this test plan documents the scope, approach and resources to be utilized for Interface Testing.

The purpose of Interface Testing is to confirm that the SDU functions according to the design, effectively communicates with interfaces and to send and receive data in accordance with all requirements. During this first phase of testing, business rules are examined and the downstream impacts are reviewed. Single points of contact will be identified for each SDU interface. The SP Test Team anticipates that the coordination and communication of Interface Test issues and their resolution will be the responsibility of the single points of contact from each of the interfacing entities. There will be a flow of information exchanged between the teams to ensure that testing issues are expeditiously identified and resolved.

Once the SP Test Team has determined that the entrance criteria is satisfied, the SP Test Team will conduct the SDU Interface Testing Readiness Review (SITRR), as required in SOW IM 3.15. Once the State has given approval to commence interface testing, the SP Test Team will execute the interface test scripts according to the processes and procedures documented in this approved Interface Test Plan.

The interface logic will undergo the same testing as other system components and will use system-generated test data based on the Participant Match File that is generated from SWS. The results of each interface test will be reported in CDL IM 009-1, Interface Test Report for each external agency and in accordance with SOW IM 3.20.

1.3 SCOPE

The Interface Testing scope for CCSAS Version 1 will include the following major components: SWS, ARS, CASES, IDB, CSR, Banking Institutions and the SDU. The SDU testing described in this document includes processing collections, reconciliation processes and generating disbursements of the support payments. Each CCSAS major component is being implemented by a different interface partner. However, each of these major components has interdependencies that need to be coordinated for the Interface Testing to be considered successful.

Due to the interdependencies, the Interface Testing calendar (Appendix B) must be planned and executed jointly with the interface partners. The SDU interfaces will be tested to determine that they are working properly. This testing will include receipt and processing of inbound data files and creation of outbound data files.

The interface testing approach is premised on the ability to receive the system generated inbound files from each of the interface partners. Inbound file testing will involve receiving and processing the interface partner's files into the SDU Interface test environment. The inbound files will be validated against the Interface Control Documents (ICDs) for content and format. The next step will be to produce outbound files from the inbound files accepted earlier in the process. The outbound file testing will involve creating and sending files produced in the SDU Interface test environment. The outbound testing will also include receiving an acknowledgement back to the SP Test Team. The detailed test scripts will contain the interface dependencies.

Interface Testing will include the following interface partners:

SWS
ARS
CASES
IDB
CSR
Banking Institutions (Mock data for inbound files-Refer to section 1.4)

The following Table 1-1 provides the detailed interfaces within the SDU indicating the source and destination systems. The following table provides a complete SDU Interface list. This table also includes the interfaces that have been deferred for the following reasons (refer to the Implementation Schedule [IM 002] for updated dates for deferred interfaces):

For the Electronic Payment Engine, Electronic Payment Card, and Credit Card Payment Processor components (including Participant and Employer Validation Data) – an agreement was reached with the State to defer this functionality until May, 2006. The CA SDU Implementation Manager worked with the State to reach the following agreement:

The SDU electronic payment engine (EPE) provides self-service capabilities (e.g., web, IVR) to payors. EPE, credit card payments and electronic payment card disbursements will not be available until after the LCSAs fully transition to the SDU in May 2006. This is consistent with the SDU Implementation Strategy as documented in the SDU Implementation Management Plan. Accordingly, testing of these functions can be delayed until later.

Foreign Currency Exchange Rates testing is deferred because at this present time, DCSS accounting has not validated that we can use a bank other than the

Misc-Sort Bank. It is deferred until further direction from the State since this is a State provided financial institution.

CSE and SDU			
Collections Engine (CE)	**Description**	**Source**	**Destination**
Participant Match File	Contains detailed information about specific records on all individuals including Custodial Parties, Non-Custodial Parents and children identified by the SWS/CSE as participants in the California IV-D program, and is used as an aid to positively identify payment information received to facilitate payment posting in SWS	SWS	SDU
Refuse Check Instructions	Contains participant information to flag certain bank accounts as no longer acceptable for submitting payments.	SWS	SDU
Suspense Notification	Contains specific information from the State detailing participants and cases in which payments are held in suspense within CSE.	SWS	SDU
Suspense Update	Contains data regarding suspended items including exceptions data identified, both resolved and updated from the daily processing.	SDU	SWS
Received Collections	Contains detailed information about specific payment records including date of payment, payment type, amount, remitter, address, Non-custodial Parent, Custodial Parties and Participant ID numbers.	SDU	SWS

Returned Collections	Contains detailed information about specific payment records that have been rejected by the bank for payment for various reasons (for example, insufficient funds, refer to maker, stopped payment, account closed, signature missing).	SDU	SWS
FMS Negative Adjustment	Contains FMS (Financial Management Service Department of the Treasury) Negative Adjustment data which details payment adjustments to the child support payments collected through the automated intercept processes.	SDU	SWS
Disbursements	**Description**	**Source**	**Destination**
SWS Disbursement Instructions	Contains the specific disbursement instructions (for example, Payee Name, Address, Date, and Amount) for all payment methods (Check, ACH Direct Deposit, and EPC [deferred]) from the SWS system.	SWS	SDU
SWS Disbursement Reject	Contains Reject Confirmation data indicating the SWS Disbursement Instruction submitted by the State that did not pass the State-Defined record/field-level edits used in assessing the validity of the Instruction.	SDU	SWS
SWS Disbursement Delete	Contains Delete Confirmation data indicating that a request to remove the Disbursement Instruction prior to the next scheduled Payment Extract event has occurred.	SDU	SWS

SWS Disbursement Origination	Contains Origination Confirmation data for the records that have been originated for a particular day, and is designed to ensure that SWS is provided with timely, record-specific information as to the disposition of Disbursement Instructions.	SDU	SWS
SWS Disbursement Status	Contains Payment Status Update information on records that have changed status. For example, a disbursement via check has changed from Outstanding to Stop.	SDU	SWS
SWS Notification of Change	Contains Notice of Change data which details information about specific ACH changes to the specific Disbursement Instructions. For example, an ACH disbursement has changed due to an incorrect routing/transit number or an incorrect individual name.	SDU	SWS
Direct Deposit Enrollment Engine (DDEE)	**Description**	**Source**	**Destination**
Enrollment/Activation/ Termination Reject (ACH/EPC) (EPC – Deferred)	Contains records that were not uniquely matched on the EAT,S file from SWS which require further review/research.	SDU	SWS
Enrollment/Activation/ Termination Status (ACH/EPC) (EPC - Deferred)	The SDU ACH/EPC Capture Interface will generate a batch file providing SWS with a framework from which to specifically update a CP's record and available disbursement method. The file will support both loading of ACH Direct Deposit instructions (for example, Bank Routing/Transit, and Bank Account) and confirmation of EPC activation.	SWS	SDU

Notice Printing Solution	Description	Source	Destination
Print Notice File	Contains correspondence instructions to be transmitted to the SP Print Facility for print production and mailing.	SWS	SDU Print Facility
Consortia (ARS/CASES) and SDU			
Disbursements	**Description**	**Source**	**Destination**
ARS Disbursement Instruction File(s)	Contains by county (San Diego, Orange, and Los Angeles), (1) Electronic Disbursement Instructions (ACH Direct Deposit – PPD/CCD); (2) IV-D Check Disbursement Instructions; and (3) IV-A Check Disbursement Instructions (for example, Payee Name, Address, Date, and Amount) from the ARS system.	ARS	SDU
CASES Disbursement Instruction File(s)	Contains the specific disbursement instructions (for example, Payee Name, Address, Date, and Amount) for all payment methods (Check, ACH Direct Deposit, and EPC [deferred]) from the CASES system.	CASES	SDU
ARS Disbursement Reject	Contains Reject Confirmation data indicating the ARS Disbursement Instruction submitted by ARS did not pass the State-Defined record/field-level edits used in assessing the validity of the Instruction.	SDU	ARS
CASES Disbursement Reject	Contains Reject Confirmation data indicating the CASES Disbursement Instruction submitted by CASES did not pass the State-Defined record/field-level edits used in assessing the validity of the Instruction.	SDU	CASES

ARS Disbursement Delete	Contains Delete Confirmation data indicating that a request to remove the Disbursement Instruction prior the next scheduled Payment Extract event has occurred.	SDU	ARS
CASES Disbursement Delete	Contains Delete Confirmation data indicating that a request to remove the Disbursement Instruction prior the next scheduled Payment Extract event has occurred.	SDU	CASES
ARS Disbursement Origination	Contains Origination Confirmation data for the records that have been originated for a particular day, and is designed to ensure that ARS is provided with timely, record-specific information as to the disposition of Disbursement Instructions.	SDU	ARS
CASES Disbursement Origination	Contains Origination Confirmation data for the records that have been originated for a particular day, and is designed to ensure that CASES is provided with timely, record-specific information as to the disposition of Disbursement Instructions.	SDU	CASES
ARS Disbursement Status	Contains Payment Status Update information on ARS records that have changed status. For example, a disbursement via check has changed from Outstanding to Stop.	SDU	ARS
CASES Disbursement Status	Contains Payment Status Update information on CASES records that have changed status. For example, a disbursement via check has changed from Outstanding to Stop.	SDU	CASES

IDB / CSR and SDU			
Standard Intercept Exchange (FMS, EDD, FTB, Lottery)	Contains intercept collection data from FMS, EDD, FTB, State Lottery and CSR including participant data, payment amounts, source, and collection dates.	IDB	SDU
CSR Collections	Contains child support payment information as a result of non-wage collection activity that includes seizure of personal property (for example, automobiles, airplanes, boats) by the California SWS/CSE.	CSR	SDU
CTS Banks and SDU			
Foreign Currency Exchange Rates (Deferred)	Contains the current foreign exchange rate valuations to the US dollar from the CTS banks, which allows for proper valuation and crediting to accounts in US dollars.	BOA	SDU
Bank of America (BOA) and SDU			
Collections and BOA	**Description**	**Source**	**Destination**
Daily ACH Credit Collections	Contains the specific payment, individual and case information and data related to the child support payments received through the ACH Network.	BOA	SDU
Disbursements and BOA	**Description**	**Source**	**Destination**
Positive Pay Check Issue	Contains the Bank of America Positive Pay Check Issue activity for loading into the Positive Pay application.	SDU	BOA

Paid Check Confirmation	Contains confirmation of payment of a Check Disbursement. This file is utilized by the SDU to update the audit trail and reflect the most current status of the Disbursement Instruction (for example, modifying the status from Outstanding to Paid).	BOA	SDU
Stop Payment Request	Contains records where the web user interface was utilized to initiate Stop activity to be loaded into the bank Stop/DDA application.	SDU	BOA
Stop Payment Request Confirmation	Contains confirmation from Bank of America of receipt of each record transmitted on the Stop Payment Request. This file is utilized by the SDU to update the audit trail and reflect the most current status of the Disbursement Instruction (for example, modifying the status from Outstanding to Stop/Void/Stale).	BOA	SDU
Void Payment Request	Contains records where the web user interface was utilized to initiate Void activity to be loaded into the bank Positive Pay application.	SDU	BOA
Electronic Disbursement Origination, PPD	Contains extracted disbursement instructions that are to be fulfilled through the electronic payment method of Direct Deposit (PPD) to be transmitted to the Bank of America.	SDU	BOA
Electronic Disbursement Origination, CCD+	Contains extracted disbursement instructions that are to be fulfilled through the electronic payment method of Direct Deposit (CCD+) to be transmitted to the Bank of America.	SDU	BOA

Electronic Disbursement Origination, CTX	Contains extracted disbursement instructions that are to be fulfilled through the electronic payment method of CTX (Corporate Trade Exchange) to be transmitted to the Bank of America.	SDU	BOA
Electronic Disbursement Returns/NOC	Contains both actual returns containing various reason codes, all of which indicate that the attempted deposit to the payee failed and Notifications of Change containing various reason codes, all of which indicate that the attempted deposit to the payee was successful, however, the State needs to update specific elements of the payment instruction for example Bank Routing/Transit Number, Bank Account Number.	BOA	SDU
Image Archive	Contains images of all checks that cleared on the previous day. The images will be loaded into an image archive and accessible through the SP's Disbursement web interface and available for viewing by State and SP resources (not the Custodial Parties).	BOA	SDU
SDU Electronic Payment Engine and Collection Engine (Internal File Exchanges)			
EPE Collections Data (Deferred)	Contains credit card collection data gathered via the SDU Electronic Payment Engine, which will be processed by the SDU Collections engine and included within collections interfaces to the State.	SDU EPE	SDU CE

EPE Returned Collections (Deferred)	Contains detailed information about specific payment records that have been rejected by the bank for payment for various reasons (for example, insufficient funds, refer to maker, stopped payment, account closed, signature missing).	SDU EPE	SDU CE
Participant Validation Data (Deferred)	Subset of Participant Match File that will include a pin for user authentication.	SDU CE	SDU EPE
Electronic Payment Engine and BOA			
EPE Originated ACH Payments (Deferred)	Contains SDU web originated EFT payment data such as debit and electronic check to be transmitted to the Bank of America for further processing.	SDU	BOA
EPE Returned Collections (Deferred)	Contains detailed information about specific payment records that have been rejected by the bank for payment for various reasons (for example, insufficient funds, refer to maker, stopped payment, account closed, signature missing).	BOA	SDU
Employers and Electronic Payment Engine			
Employer Validation Data (Deferred)	Contains EFT Payment data from Employers paying on behalf of an employee. This data originates from the SDU application made available to employers to transmit payment information for multiple employees at one time.	Employers	SDU EPE

Disbursements Engine and SDU IVR			
Disbursements History	Contains specific disbursement historical data for access via the SDU IVR and web by enrolled and authenticated participants.	SDU DE	SDU IVR
Disbursements Engine and SDU Print Facility			
Check Disbursement Origination	Contains disbursement instructions that are transmitted to the Print Facility for print production and mailing.	SDU	SDU Print Facility
Check Disbursement Confirmation	Contains confirmation of receipt of each Check Disbursement Origination and is utilized by the SDU to update the audit trail and reflect the most current status of the Disbursement Instruction (for example, modifying the status from Issued to Outstanding).	SDU Print Facility	SDU
SDU Electronic Payment Engine and Credit Card Payment Processor (CCPP)			
Credit Card Payments (Deferred)	Contains standard commercial banking services for credit card payments.	SDU EPE	CCPP

Table 1-1 System Source and Destination

1.4 BANKING INSTITUTION INTERFACE TESTING

The SDU Interface Testing as described in this document will not include end-to-end testing with the Banking Institution. Specifically, this means that the SDU testing will create the test files that would be sent to or received from the Banking Institution, but the actual transfer will not occur. The SP Test Team will evaluate the output files for accuracy of format and content. Mock input files will be used to process incoming Banking Institution data. The reason for this approach is because the SDU is using standard commercial banking services. These services are used throughout the banking industry, and the SDU is acquiring these services. A standalone test of these services will be performed at a later date in the implementation. The testing for Banking Interfaces will be performed during System Qualification Testing timeframe at our production facility.

2.0 DEFINITIONS

Table 2-1 defines the terms used in this Interface Test Plan.

Term	Definition
Application	The complete build of all SDU subsystems.
Defects	Nonconformance to requirements. Also known as anomaly, bug, error, exception and fault.
Interface Control Documents (ICD)	The individual definitions of each interface within the IID.
Interface Design Description (IDD)	A description of the interface design.
Interface Implementation Descriptions (IID)	A description of the interfaces between the SP and the interface partners.
Interface Partners	ARS, SWS, CASES, IDB, CSR, and Banking Institutions
Regression Test	The selective retesting of components that have been modified to help ensure that any defects have been fixed and that newly added features have not created new defects with previous versions of the software.
Requirements Traceability Matrix (RTM)	The Requirements Traceability Matrix is a representation of user requirements aligned against system functionality. It is used to ensure that all requirements are being met by the system deliverables.
SDU Interface Testing Readiness Review (SITRR)	SDU Interface Testing Readiness Review. This review is used to verify that all required components and work products have been completed so that Interface Testing can begin.
State	Department of Child Support Services (DCSS) and Franchise Tax Board (FTB)
Test Condition	A specific test (or validation) executed within a test script. Test conditions are verifiable checkpoints that are performed during the execution of a test script to determine test success or failure. A test condition may be stated in terms of an expected result.
Test Cycles	Logical groupings of related test scripts to facilitate test execution.
Test Data	Any data that is used as input, output or in the execution of a test script.

Term	Definition
Test Execution	The process of performing the actual test itself, as defined during the Test Preparation activity for each type of test. Includes performing the test, documenting actual results, marking the test as Passed or Failed, evaluating the test results, entering defects as necessary, regression testing and test progress status reporting.
Test Requirement	Identified testable requirements in the RTM derived from the RFP, SP proposal, requirements documentation and other appropriate SDU product descriptions.
Test Scenario	A series of activities that follow a business process and may result in several test scripts or be combined in one test script. Test Scenarios are events that are grouped together for a particular business requirement.
Test Script	A series of test steps that follow a business process. Test scripts, which contain test conditions that are validated within the script, are organized into test cycles.
TestTrack Pro™	Defect tracking software used by the SP for test management and defect management.
Visual SourceSafe	The software configuration management tool.

Table 2-1 Definitions

Table 2-2 defines the SP Acronyms used in this Interface Test Plan.

SP Acronym	Term
ACH	Automated Clearing House
BOA	Bank of America
CCPP	Credit Card Payment Processor
CE	Collections Engine
CIE	CORE Interface Engine
CORE	Collections, Operations, and Reconciliation Engine
DDEE	Direct Deposit Enrollment Engine
DE	Disbursement Engine
EPC	Electronic Payment Card
EPE	Electronic Payment Engine
ICD	Interface Control Document
PMF	Participant Match File

SP Acronym	Term
SDU	State Disbursement Unit
SITRR	SDU Interface Testing Readiness Review
SP	Service Provider

Table 2-2 SP Acronyms

3.0 RELATED DELIVERABLES

Deliverable Identifier	Deliverable Name
IM 001	Implementation Management Plan
Relationship to the Interface Test Plan: This deliverable provides project management methodologies, tools and procedures used in the interface testing process. This document was used throughout the descriptions in this test plan since much of the information was already submitted to the state, and subsequently approved.	
IM 002	Implementation Schedule
Relationship to the Interface Test Plan: This deliverable is used as input for creating the Test Schedule in Appendix B.	
IM 005	Interface Implementation Description (IID)
Relationship to the Interface Test Plan: This deliverable describes the interface between SWS, ARS, CASES, IDB, CSR and the SDU. Due to the delivery of IM005 occurring following the delivery of IM 008, the SP has been coordinating the interfaces contained in both documents so that the interfaces remain consistent.	
IM 009-1	Interface Test Report
Relationship to the Interface Test Plan: The results of each interface test will be reported in the Interface Test Report. These reports are produced as a result of the procedures presented in this test plan.	
OM 006	SDU Security Plan
Relationship to the Interface Test Plan: This deliverable describes the Security processes and procedures used to implement physical and system security. Due to the delivery of OM 006 following the delivery of IM 008, the SP included a table that describes how each of the RFP requirements for this document as related to Interface Testing.	
TM 010	Problem Resolution Management Plan
Relationship to the Interface Test Plan: This document describes the defect definitions and descriptions. The State indicated during the creation of IM 001 that there needs to be a consistent defect classification and prioritization for all interface partners. Therefore, the SP used the approach used in TM 010 verbatim in IM 001 and has repeated the same approach in this test plan.	
TM 029	SDU Integration Plan
Relationship to the Interface Test Plan: This document was used to provide additional detailed information surrounding the development and testing of the CSE/SDU Integration from the perspective of SWS.	

Deliverable Identifier	Deliverable Name
TM 030	CSE/SDU IDD
Relationship to the Interface Test Plan: The CSE/SDU IDD documents the data exchange requirements between SWS and the SDU. It describes the SDU interface of the CCSAS CSE system and will be used to validate the interface and prepare test data. The IDD was referenced in developing the scripts. The IDD has undergone changes, and hence the SDU ICD's and internal IID's were then used to develop the final validation points within the scripts.	
TM 032	Master Test Plan
Relationship to the Interface Test Plan: The Master Test Plan provides the high level overview of External Entity testing within the CCSAS CSE system, including a discussion of the CCSAS interface testing responsibilities. This document was referenced when defining the roles and responsibilities section in this test plan.	

Table 3-1 Related Deliverables

4.0 ASSUMPTIONS

The test Participant Match File provided by the BP will contain a representative sample of participants in a large enough number to generate unique test payment transactions for each phase of testing.

Interface Partner resources are available for Interface Testing. A contact person for each entity is assigned to receive and process the data. Section 6.1 describes the Interface Partners involved in Interface Testing.

Each interface partner will be able to participate and support the SDU Interface Testing by processing the files generated by SDU system as well as providing system generated files for SDU processing.

Each interface partner will process and validate all outbound files from the SDU and report any defects back to the SDU.

Defects identified by the interface partners during the SDU Interface Testing will be prioritized by the interface partner and fixed in a timely manner that will allow for retesting of the test scripts.

5.0 DOCUMENT MANAGEMENT

The Interface Test Plan will be placed in the document management tool, the SDU eRoom, and will be subject to version control. Additionally, the State will place the document in the CCSAS Library.

Changes to this document will follow the project guidelines for delivery and communication to the appropriate State Representative. The detailed changes to this document will be noted in the List of Revisions section.

6.0 IDENTIFICATION AND DESCRIPTION

6.1 INTERFACE PARTNER TEST APPROACH

This section provides an overview of the Interface Partner testing approach for interface testing, Version 1.

For the purposes of this section, an *Interface Partner* may denote one of several types of interfaces:

- **Private Sector Entity Interfaces:** These are interfaces with nongovernmental entities such as banking institutions.
- **Public Sector Entity Interfaces:** These are interfaces with other states' collections and disbursements
- **CCSAS Interfaces:** These are interfaces within the CCSAS architecture, including the interfaces between the SDU and SWS, ARS, CASES, IDB and CSR.

In general, there are three key aspects for testing each interface that need to be considered:

- **SDU Processing** – This includes the file creation process for outbound interfaces and the programming logic to process the inbound interfaces.
- **Transport** (if available) – This includes the procedures, technology and processes to move files from one system to another. The transporting of files will be tested during Interface Testing when the processes and technology are established by the State, SP and Interface Partners. For outbound interfaces, this takes the file from the SDU system to the interface partner. For inbound interfaces, this refers to how the file moves from the interface partner to the SDU system.
- **External Validation/Processing** – For outbound interfaces, the SP Test Team provides validation of the file produced by the SDU system. The interface partner then validates the format and content of the file created and if possible, processes the file in a test environment for the receiving system. For inbound interfaces, this involves testing a file that is created by the interface partner in their test/QA environment. The SP Test Team will validate the file produced by the Interface Partner.

6.2 ROLES AND RESPONSIBILITIES

The following table, 6-1, defines the roles and responsibilities of the teams during Interface Testing.

Team Name	Interface Test Role
SDU Solution Configuration Team	• Provide technical support • Fix documented defects • Produce unit test releases • Support regression testing
SP Test Team	• Develop major sections of the Interface Test Plan with the exception of coordination with interface partners • Develop Test Scenarios and Test Scripts • Coordinate internal SDU Interface test execution activities • Coordinate internal SDU Interface regression testing • Develop the Interface Test Report • Validate and record test results in the test tracking tool
SP Testing Support Team	• Prepare and lead SITRR discussions with State • Develop Interface Test Plan by: o Defining the content for the Interface Test Plan o Providing content for sections related to Interface Partner Coordination o Communication of Testing Progress to the Interface partners o Review and compile the contents of the Test Plan • Test Scenarios and Scripts: o Review the Test Scripts and Test Scenarios for compliance with the IID requirements o Identify gaps Package Test Scripts and Scenarios for submission to the state and Interface partners • Coordinate the Testing Schedule with each Interface partner • Validate test results in the test tracking tool • Coordinate the execution of the tests and exchange of files with interface partners • Coordinate with SP Test Team and Interface partners to prioritize and retest defects • Communicate the resolution of all Interface-related defects to interface partners • Produce reports to share with the State and Interface Partners on the progress of testing • Coordinate all testing efforts for Interface Testing

Team Name	Interface Test Role
Interface Partners	• Responsible for facilitation and coordination of Interface test planning, execution and validation activities between the Interface partner and the SP Test Team • Report on the processing of outbound files from the SDU • Coordinate the transmission of SDU related inbound files • Report on defects identified on their system during testing, and coordinate with SP Test Team for prioritization, resolution and retest of identified issues • Participate in Test Meetings organized by the State
State Support Team	• Assists the SP Test Team in coordinating Interface Testing activities with all Interface partners • Review progress on Interface testing and resolve testing related issues • Coordinate Test Meetings with Interface Partners to obtain status, discuss file exchange schedule, jointly prioritize defects and plan for retests.

Table 6-1 Roles and Responsibilities

6.3 ROLES AND RESPONSIBILITIES BY TEAM AND POSITION

The following table defines the roles and responsibilities of the teams by position as it relates to SDU Interface testing and Interface partners.

Role/Team	Testing-Related Responsibilities and Involvement
SP Solution Configuration Team Roles:	
Technical Manager	• Manages all interface design and documentation • Manages the coordination between the Solution Configuration Team and all other testing partners • Responsible for coordination of the setup and configuration of testing tools and software
Technical Lead	• Manages Interface testing of each subsystem • Coordinates with SP Test Team during interface testing to address defects • Coordinates release schedules and regression testing activities with the SP Test Team
Developer	• Analyzes software to diagnose and fix defects

Table 6-2 Solution Configuration Team Roles

Role/Team	Testing-Related Responsibilities and Involvement
SP Test Team Roles:	
Test Manager	• Manages development of Interface Test Plan (CDL IM-008-1) • Sets/Refines overall Interface testing strategy and procedures • Responsible for completion of test preparation and execution activities • Provides oversight and support for the Test team members • Conducts and participates in planning and on-going status meetings • Overall Responsibility for test planning, preparation, execution and development of Interface Test Report (IM-009-1) • Establishes/reviews procedures to load test data into the test environments • Performs testing Quality Control (QC) activities, including: o Verifying test script traceability o Verifying regression testing o Validating exit criteria and providing input to the build process • Publishes and analyzes testing metrics to identify potential bottlenecks in test execution or defect resolution processes • Responsible for communicating and ensuring test issues are addressed
Test Lead	• Conducts test planning activities • Provides oversight, guidance and support for the test team • Performs testing quality control activities, including: o Verifying test script traceability o Verifying regression testing o Validating exit criteria o Performing metrics collection and analysis • Plans and conducts ongoing status meetings • Provides input for testing tool setup and *TestTrack Pro*™ for defect tracking • Leads and executes tests for Interface Test, including: o Test script execution o Documentation of actual results o Pass/fail assessments • Follows procedures and supports the Test team in the use of testing tools and Problem Resolution Management tool for defect tracking • Creates and contributes to testing deliverables and work products • Performs any necessary test work product changes • Coordinates with Test Manager to establish and follow procedures

Role/Team	Testing-Related Responsibilities and Involvement
	to load test data into the test environments • Publishes and reviews metrics to identify potential bottlenecks in test execution or defect resolution processes • Responsible for communicating and ensuring test issues are addressed • Works with the Technical Manager to validate that the system and software requirements are appropriately reflected in test conditions and test scripts • Provides functional support for Interface Test team
Tester	• Plans test execution and defines test conditions, test scripts and scheduling for own area of testing responsibility, following test procedures and planning documentation • Documents traceability between the functional requirements to test scripts • Utilizing appropriate test tools, capture, document and record test activities • Responsible for execution of Interface Tests, including: o Test script execution o Documentation of actual results o Pass/fail assessments • Records defects, reviews resolution of defects and performs regression testing • Participates in Problem Resolution

Table 6-3 Test Team Roles

Role/Team	Testing Related Responsibilities and Involvement
SP Testing Support Team	
Testing Oversight Manager	• Oversee interface testing • Work with the testing team to validate the test approach • Supervise the creation of test scripts and test plans • Responsible for all testing activities, including: o Test plan development o Test coordination o Test script development for Interface Testing • Report on the results of testing conducted by the SP • Oversee the testing staff for all aspects of testing and test coordination • Resolve testing related issues • Track the progress of test planning, execution and validation efforts • Manage all risks associated with Interface testing

Role/Team	Testing Related Responsibilities and Involvement
External Test Support Manager	• Defines the content of the Interface Test Plan; reviews content provided by the Test Lead for the Test Plans and identifies gaps; develops content for portions of the Interface Test Plan as it relates to Interface Partner Coordination, communication with interface partners, reporting progress of testing related activities • Responsible for facilitation and support of Interface Testing with all interface partners • Identifies and reports on all testing-related issues and risks • Coordinates with the appropriate interface partners to prioritize and retest defects • Sets/refines overall testing strategy with the State • Responsible for completion of test planning, preparation and coordination of Interface test execution activities • Provides oversight and support for the Testing Support team members • Conducts and participates in planning and on-going status meetings • Responsible for reviewing the setup and configuration of testing tools and software • Reviews/escalates problems as defined in the Testing Section of IM001 (Implementation Management Plan) • Prepares and leads SITRR discussions with the State • Performs testing Quality Control (QC) activities, including: • Verifying test script traceability • Publishing and analyzing testing metrics • Identifying potential bottlenecks in test execution, defect creation or defect resolution processes • Providing the status of testing-related progress to all interface partners • Addressing all testing-related issues
Senior Test Support Lead	• Reviews and comments on Interface test planning and oversight activities • Facilitates testing QC activities • Reviews traceability of test scripts • Reviews exit criteria and provides input to the build process to support the execution of tests • Facilitates metrics collection and analysis • Facilitates the development of detailed test plans for interface testing in partnership with the Testing Team • Coordinates the execution of the tests and exchange of files with interface partners • Facilitates planning of ongoing testing status meetings • Reviews input for setup and configuration for testing tools and

Role/Team	Testing Related Responsibilities and Involvement
	software • Facilitates and coordinates external test planning activities for Interface Test, including: o Test conditions o Test scripts o Test cycles o Data-related activities o Test scheduling • Coordinates the execution of the tests with the Test Team for Interface Testing • Coordinates with SP Test Team and Interface partners to prioritize and retest defects • Contributes to testing deliverables and work products • Facilitates and reviews any necessary test work product changes • Publishes and reviews metrics to identify potential bottlenecks in test execution, defect creation or defect resolution processes • Responsible for documenting test issues that are identified by the SP Test Team • Conducts Quality Assurance (QA) to help ensure that system and software requirements are appropriately reflected in test conditions and test scripts • Responsible for test preparation and planning for Interface Testing
Tester Support	• Supports the development of test scenarios and scripts that cover interface testing • Conducts Quality Assurance (QA) to help ensure that system and software requirements are appropriately reflected in test conditions and test scripts • Supports the test execution with Testing Team for interface testing • Utilizes appropriate test tools, capture, document and record test activities • Supports the development of Interface Test Report • Support the testing execution, such as: o Test script execution o Documentation of actual results o Pass/fail assessments • Participates in Problem Resolution

Table 6-4 Test Support Team Roles

Role/Team	Testing Related Responsibilities and Involvement
State Support Team	
State Test Lead	• Assists the SP Test Team in coordinating Interface Testing activities with all Interface partners • Review progress on Interface testing and resolve testing related issues • Coordinate Test Meetings with Interface Partners to obtain status, discuss file exchange schedule, jointly prioritize defects and plan for retests.

Table 6-5 State Support Team Roles

Role/Team	Testing Related Responsibilities and Involvement
Interface Partner Contact	
Interface Partner Contact (SWS, ARS, CASES, IDB and CSR)	• Responsible for facilitation and coordination of Interface test planning, execution and validation activities between the Interface partner and the SP Test Team • Report on the processing of outbound files from the SDU • Coordinate the transmission of SDU related inbound files • Report on defects identified on their system during testing, and coordinate with SP Test Team for prioritization, resolution and retest of identified issues • Participate in Test Meetings organized by the State • Coordinate with respective internal teams to schedule retest of defects and associated scripts on resolution of SP Interface related defects

Table 6-6 Interface Partner Contact Roles

6.4 Coordination and Planning with Interface Partners

This subsection identifies and describes the approach to planning and coordinating SDU interface activities with the following interface partners:

- SWS
- ARS
- CASES
- IDB
- CSR
- Private (e.g. Banking Institutions, etc.)
- Public (e.g. local, state, and federal government)

6.4.1 Overall Approach

The following is the SP approach to planning and coordination of SDU interface activities with: SWS, ARS, CASES, IDB, and CSR. Early planning and coordination

activities with all interface partners is essential to the SP Interface testing. The SP Test Team has developed a test schedule for each of the file exchanges that are going to be tested as part of the Interface Testing phase. This schedule has been reflected in the IM002 deliverable. The SP Test Team developed detailed test scenarios and test scripts for each of these interfaces. These test scripts are organized into a Test Cycle and a detailed test calendar (refer to Appendix B) that is in alignment with the test schedule reflected in IM002 at the time of the publication of this document. It is anticipated that IM002 will be updated on a regular basis . Appendix B is a representation of the most current test calendar and has been adapted to meet the needs of Interface Partners.

The SP Test Team will work with the State to coordinate meetings with representatives from SWS, ARS, CASES, IDB and CSR. During these planning meetings, the SP Test Team will share the detailed test calendar with each of the Interface Partners and discuss the SP expectations as it relates to testing and validation of results. This will allow the Interface Partners the ability to plan their activities for the testing and processing of files sent to and received from the SP Test Team. As reflected in IM002, the SP Test Team is conducting multiple rounds/cycles of test for each of the interface files with the interface partners.

The SP Test Team also recognizes that regular communication will be required with each of the interface partners during interface testing. The SP Test Team will use the communication mediums, processes and procedures that have already been established by the State.

In addition, the SP Test Team will work with the State and interface partners on the processes that are needed to ensure a smooth transition for all parties. This includes defining a formal FTP file transfer process for interface files that will apply to all interface partners that are related to the SDU.

6.4.2 Interface Readiness Reviews

Once the SP Test Team has determined that the Interface Testing entrance criteria is satisfied, the SP Test Team will conduct the SDU Interface Testing Readiness Review (SITRR), as required in SOW IM 3.15.

The SP Test Team will work with the State to prepare for the SITRR. During these meetings, a review of the testing calendar as it relates to interface testing will be solidified and processes will be discussed to ensure proper follow through of the set activities and dates. The SP Test Team and the State will work together to develop the checklist for the Interface Readiness Reviews. This will include at a minimum all of the entrance criteria that has been included in the test plan.

Any resulting Action Item from the SITRR will be tracked to resolution through the SP PMO Action Item Process.

In preparation of the SITRR, the SP Test Team will provide an agenda in advance of the actual meeting day to conduct the review. The SP Test Team will conduct the

SITRR with the State and other relevant stakeholders before the actual execution of any interface tests.

Once the State has given approval to commence Interface testing, the SP Test Team will execute the interface test scripts in accordance with the Interface Test Plan.

6.4.3 Reporting Progress/Communication to the State and interface partners

Progress on Interface Test planning and execution will be communicated during regular weekly meetings with the State and interface partners. During these recurring weekly meetings, the SP Test Team will inform participants of test planning progress, preparation, and issues related to interface testing. The SP Test Team participates in the Integrated Test Team meetings where representatives from ARS, CASES, SWS, CSR, and IDB are present to ask questions regarding interface testing and other related areas. During the Integrated Test meetings, the SP will provide an update on test planning, execution and issues. Weekly, the SP Test Oversight Manager and External Test Support Manager meet with a State representative to discuss specific issues or questions that surround testing. In this forum, questions and concerns can be raised to the State directly and then communicated to partners if applicable. During the weekly Interface discussion meetings, interface partners report on the status of interface file development with all participants. The SP External Test Support Manager will give a specific interface status during this meeting on the files that were exchanged in the previous week, along with soliciting feedback on files that the SP has sent to the interfaces partners. Should issues arise that cannot be satisfied during one of the three weekly testing meetings with Interface Partners, ad-hoc meetings will be arranged with the relevant partners to promptly and efficiently address issues impacting schedule and objectives. These ad-hoc testing meetings will be coordinated through the State to applicable parties.

Informal communication will be conducted through emails and telephone conversations with the State to help clarify any issues that arise during interface testing. The State will then communicate any applicable issues or questions to the appropriate interface partner. Any communications between the SP and Interface partners, except for Banking Institutions, will include in the distribution list at least one State representative.

These communications will help the project stay in alignment towards meeting the objectives and schedule.

6.5 Timing, Location and Frequency of File Exchange Coordination

This subsection identifies and describes the coordination of timing, location and frequency of the file exchanges with the following interface partners:

- SWS
- ARS

- CASES
- IDB
- CSR
- Private (e.g. Banking Institutions)

6.5.1 Timing and Frequency of File Exchanges with interface partners

The timing and frequency of file exchanges will follow the established dates as stated in the Implementation Schedule submitted monthly to the State. Needs may change over the course of test preparation and testing. As a result, changes will be communicated to applicable interface partners during the various weekly testing meetings, directly to the State via e-mail or phone conversation or during other ad-hoc meetings that apply to interface testing. These changes in schedule and frequency will be reflected in the updated IM 002 Implementation Schedule submitted to the State. In addition, the SP Test Team has identified specific dates for exchange of files and which is reflected in the Test Calendar in Appendix B. This Test Calendar based on discussions with the Interface partners.

6.5.2 Single CONTACT Point for each Interface Partner

It is important to have clear lines of communication between the SP and each interface partner that the SDU will be interfacing with. To ensure that all partners receive the highest quality of response and information sharing, the SP Test Team will have point people for each interface partner along with one alternate person to fill in when necessary. By assigning individual people on the SP Test Team to each entity's interface, we will be able to provide focused feedback and assistance for all interface exchanges that will occur over the duration of the implementation.

The SP Point person for each interface will directly coordinate and communicate with each interface partner. The single point of contact will keep the SP Management team informed of all communication and progress around test planning, coordination, execution and validation activities.

The single point of contact list was distributed during the Interface Partner Coordination Meeting in preparation for the Interface Readiness Review and is also available on demand.

6.5.3 File Transfer Protocol (FTP) with interface partners

During Interface Testing, the SP will use F-Secure SSH® to exchange data with each CCSAS data exchange partner, as well as internally to our Collections and Disbursements engines located in Michigan and Colorado. The F-Secure SSH® Server will reside in our Cincinnati, OH Data Center and be accessible via the Internet. F-Secure Clients have been loaned to the CCSAS data exchange partners as needed. The F-Secure SSH® data exchange architecture and data flow is depicted in the following diagram:

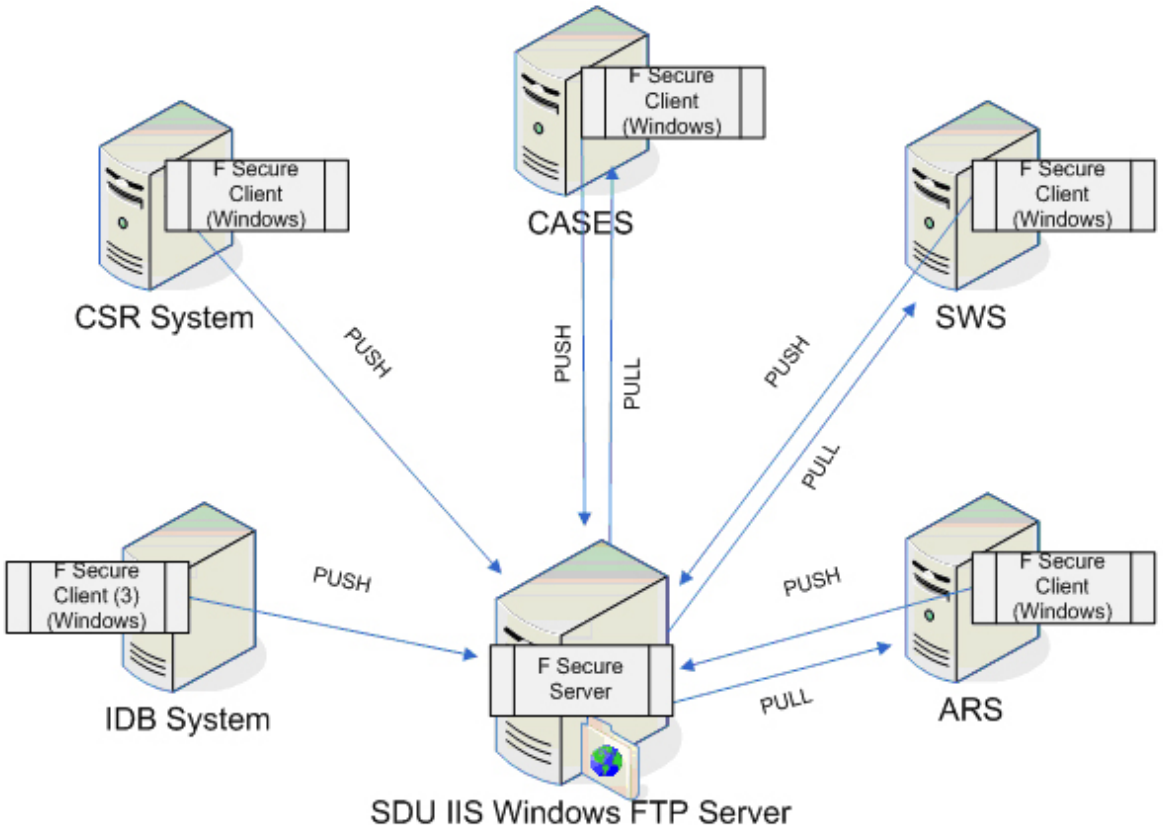


Figure 6-1 F-Secure SSH® data exchange

The F-Secure SSH® security architecture is discussed in Section 15.1 Data Security within the Environment, and an F-Secure SSH® datasheet can be found in Appendix D.

Furthermore, given the minor possibility that the secured FTP process is not in place by 4/4/05, an interim process will be used until the formal FTP process is completely established.

The interim process is as follows:

INTERIM FILE EXCHANGE PROCESS WITH INTERFACE PARTNERS

As we have done during the “Mock” data file exchange process, all interface files from SWS, ARS, CASES, IDB and CSR will be placed in specific SP folders on the AIX box (on the State servers). These files will be picked up by a HHSDC System Administrator then encrypted and password protected using WinZip 128 bit encryption. These encrypted and password protected files will be sent via e-mail to the appropriate SP development contact person. It should also be noted that the password will conform to CSE standards for password establishment. Once the file is sent, the HHSDC Administrator will call the appropriate SP development contact person with the password. Voicemail messages are also acceptable for password

exchanges. This process will be followed in reverse for files sent by the SP to the various interface partners that are expecting files from the SDU.

With each exchange of a file, a File Transmittal Form (FTF) will accompany test files that are exchanged and communicated with external entities when files are sent via e-mail from the SDU or sent from external entities to the State to be disbursed to the SDU. The FTF will accompany the file submitted to ensure proper handling and recording of all files exchanged. The FTF will contain relative information regarding the file(s) that are exchanged. Each FTF can be associated to a single file or multiple files. The form is broken down into three main sections – File Information, Transmitter Information, and Recipient Information.

File Information: This will include the name of the file(s), date the file was transmitted, transmittal time, file origination that includes the complete file path, and a brief description of the file.

Transmitter Information: This will include information pertaining to the name of the person that is sending the file, date, time transmitted, file origination that includes the complete file path, and a brief description of the file.

Recipient Information: This will contain information regarding the recipient name, institution/organization and I.D. number, title, and contact information.

6.5.4 Communication Process When Files are Not Received

The process of communicating when files are not received will be coordinated and established by the State and with the SP Test Team conforming to this process. This process should provide a standard protocol that will result in immediate resolution if a situation arises where files are not received. In the event that a file is not received through the file transfer process, the intended recipient will notify the State that the file has not been received via e-mail or by phone. Notification of files that are not received can also be discussed during the various weekly testing meetings that interface partners attend. If resolution is not obtained through the aforementioned methods, then an escalation procedure will be followed. This procedure will involve the SP Test Team contacting the State testing lead to help identify the cause of the missing file with the appropriate interface partner. The SP Test Team will provide to the State the date and file name that was planned for exchange. If the Interface Partner executed the file exchange, they will attempt a resend of the intended file, along with forwarding the original file transfer information to the intended file recipient:

The transmitter of the file(s) will verify and send the following information to the SP Test Team regarding the transference of files in the event that the files were not received:

- Date and time file was transferred
- Transfer location
- Contact personnel (recipient)

The file will be resubmitted to the intended recipient by the point of contact for the transmitting team.

6.5.5 Data Validation of Files Exchanged

Each file that is sent to the SP will be validated against file specifications and requirements gathered for each interface. Along with a general review of the requirements for the interface file, the data integrity of the system will be validated through the execution of the test scripts. The success of the tests will be measured by examining the actual results with the expected results. If there is any discrepancy, it will be reported as a defect and will follow the defect reporting procedures in TestTrack Pro™ as described in Section 12.

6.5.6 Communication on Test Scripts that have been Executed

The results of the test scripts executed during each test scenario will be provided to the State. The results will be presented in various reports as required by the State in SOW IM 3.11 and as listed in IM 001. In addition, the SP Test Team will provide a weekly test progress report to the State before the weekly integrated test meeting. The weekly SP Test Progress Report will contain but is not limited to the following:

Summary and Status of past week's work: This provides a summary and gives a status of SP testing related items for the previous week.
Significant Items or Issues that will Impact Schedule or Work: This summarizes any significant items or issues that will impact the SP's ability to stay on schedule or that will affect the progress of testing.
Accomplishments: This lists the key accomplishments of the week including major milestones completed or key tests.
Outstanding and New Work Products: This lists any outstanding or new work products that the SP is responsible for. This includes any interface files or other documentation that is required to the State or interface partners.
Upcoming Priorities within the Next Week: This lists the planned testing activities that the SP will conduct in the next week
Testing Metrics (Once Testing Begins): This section will show in either chart form or in diagrams the testing progress of the SP.
Defects
Requirement Coverage
Number of Tests Completed

After the completion of test scripts for a specific subsystem or component, the SP will make the scripts available to the State.

6.5.7 Defect reporting and Test Execution

Defects encountered during test execution will be tracked. Defects that are encountered due to an interface error that is not caused by the SP will also be tracked in our test defect tool, *TestTrack Pro*™. The SP Test Team will

communicate these defects to the appropriate party that is responsible for the defect and track the defect resolution process and assign defect prioritization within *TestTrack Pro*™. Should an interface partner discover a defect in a file that the SP sends to them, the SP Test Team will submit this defect into the tracking tool and track the defect in the same manner as if the SP Test Team encountered the defect during normal Interface Testing.

The SP has a defined Severity and Prioritization methodology as described in Section 12.1.1 of this document and which will be followed for all defects. When a defect is discovered by the SP on an inbound interface file, the SP will work with the Interface Partner to assign a prioritization level to that defect. Upon the resolution of the defects that stem from files sent or received to/from an Interface Partner, we will coordinate with the interface partner to schedule the retests of the scripts affected by the defect.

7.0 DIAGRAMS

7.1 OVERVIEW

The purpose of this section is to provide an overview of the SDU system. The intent of this overview is to provide the reader general understanding of the different components that will be included during the testing activities.

7.2 SDU COLLECTIONS, OPERATIONS, AND RECONCILIATION ENGINE (CORE) OVERVIEW DIAGRAM

The diagram below provides a high level overview of the primary subsystems and interfaces within the SDU. This diagram is not intended to represent every data or user interface within the SDU architecture, but to provide a high level overview of the internal and external relationships between SDU subsystems and corresponding interface partners.

California SDU CORE Overview

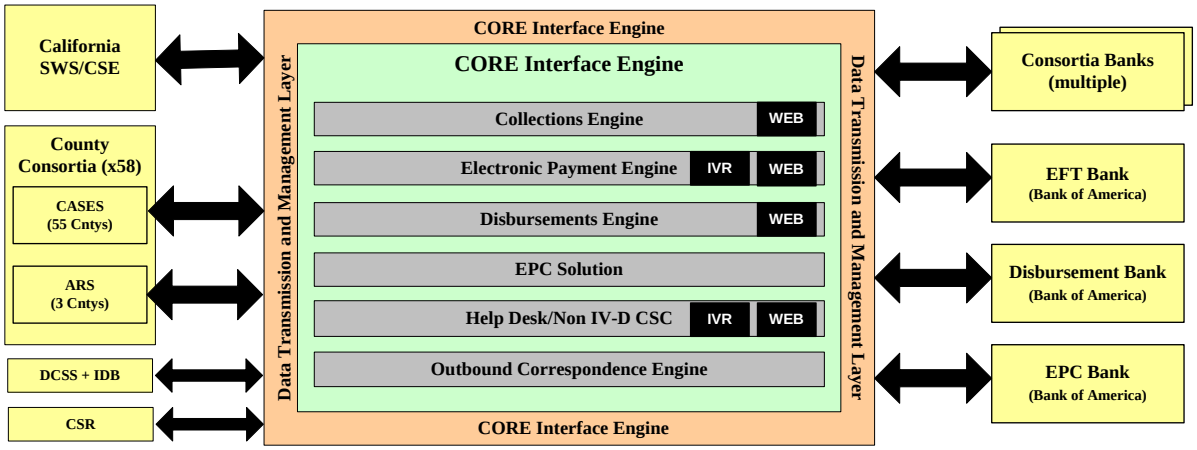


Figure 7-1 Solution Diagram

Sections 7.2.1 to 7.2.7 are included to provide a high-level description of the primary subsystems for the SDU.

7.2.1 COLLECTIONS ENGINE

The Collections Engine (CE) is the primary subsystem of the SDU for processing paper and electronic payments. This module will work in conjunction with high speed scanners to image and capture data on all physical items that come to the SDU, as well as import and capture all EFT collections.

7.2.2 ELECTRONIC PAYMENT ENGINE (DEFERRED)

The Electronic Payment Engine (EPE) is the primary subsystem for processing telephone and web-based electronic payments from employers and NCPs for the

SDU. This module will provide an Interactive Voice Response (IVR) and web interface with a robust engine to capture payments from employers and NCPs. Electronic payment requests will be converted into ACH payments and processed through the CE. All payments will be included in the daily collections file for transmission to SWS.

7.2.3 Disbursements Engine

The Disbursements Engine (DE) is the primary subsystem for managing all disbursements for the SDU. The DE will receive instructions files from SWS, CASES and ARS in Version 1. The functionality of the DE is to manage the creation and routing of files to print checks, send instructions for direct deposit and instructions for Electronic Pay Cards (EPC) (EPC deferred). The DE also provides a web-based point of access for authorized State and Local Child Support Agency (LCSA) users to view and manage disbursement activity as needed. This interface includes such services as void/stop/cancel payment capability, payment status and paid check image access.

7.2.4 EPC Solution (Deferred)

The EPC solution provides capability to give Custodial Parents (CPs) the option of receiving disbursements on a branded card, similar to a bank debit card. The EPC solution interfaces closely with the DE and SWS. This capability includes IVR and customer service support..

7.2.5 Help Desk/ Non IV-D Customer Service Center

The SDU includes an electronic help desk for stakeholders involved in electronic collection and disbursement methods, as well as a Customer Service Center to support Non IV-D participants. This component of the SDU includes IVR features, as well as an informational web site.

7.2.6 Outbound Correspondence Engine

The Outbound Correspondence Engine manages the generation and printing of all required notices and forms.

7.2.7 Data Transmission and Management Layer – CORE Interface Engine

This component will administer and control all data files passing into and out of the SDU.

The following diagram, Figure 7-2, details the subsystems and interfaces within the CASDU.

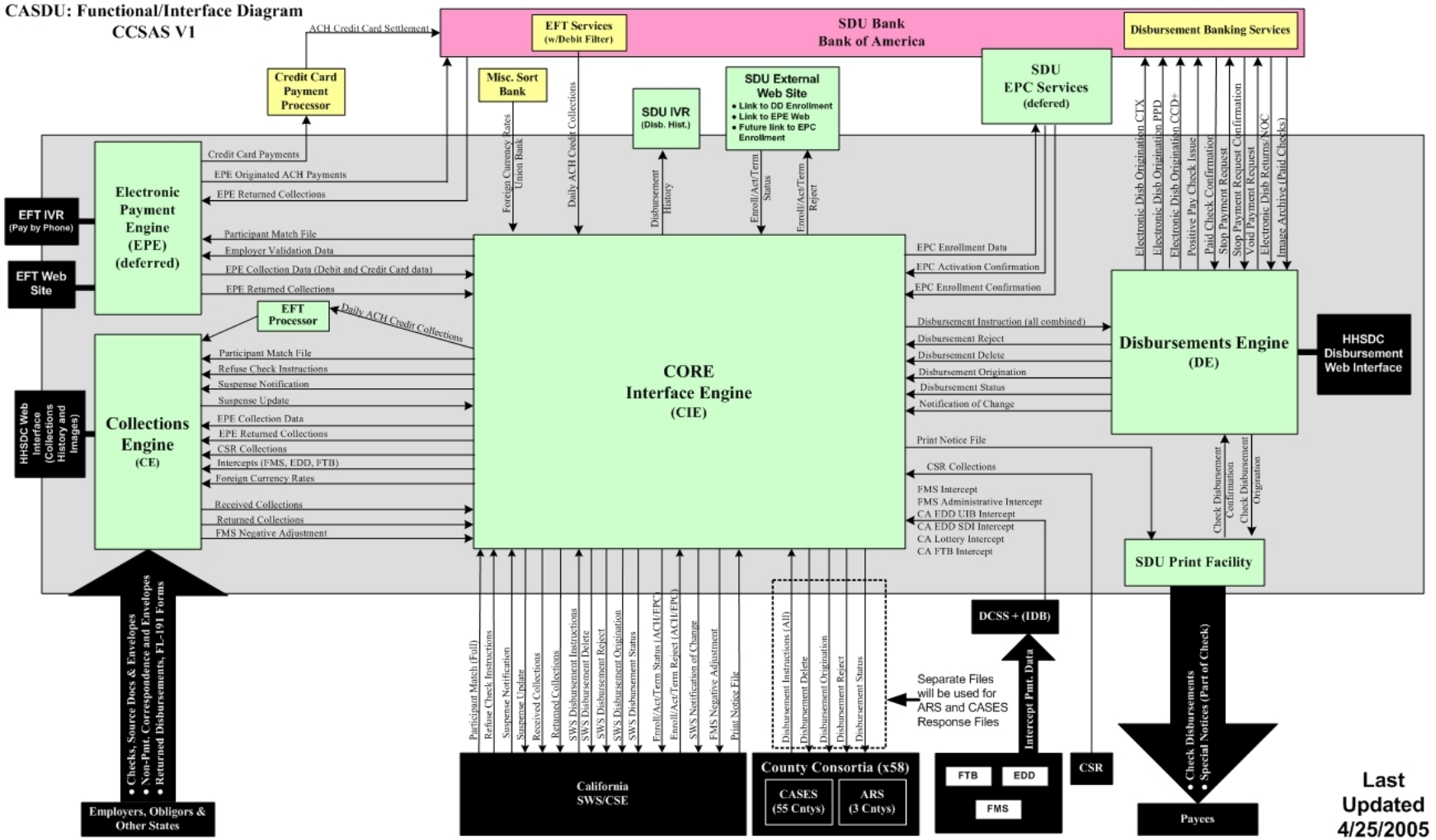


Figure 7-2 SDU Subsystems and Interfaces

8.0 DESCRIPTION OF INTERFACE TEST CRITERIA

8.1 ENTRANCE AND EXIT CRITERIA

This subsection defines the entrance criteria and exit criteria for Interface Testing. The SP Test Oversight Manager will be responsible to ensure that all entrance and exit criteria have been met.

Entrance Criteria:

- Interface Test Plan has been completed and submitted to the State for approval
- Detailed Test Schedule set up and coordinated with interface partners
- Test environment has been configured for all software and hardware (this includes security features).
- Interface Test Scripts have been written and reviewed internally
- Test Scripts have been mapped to the Requirements Traceability Matrix
- All required initial files have been received to properly populate the test environment.
- Required test data has been generated
- Test Tracking tool has been installed and configured
- Interface Readiness Review has been conducted and approval has been received to proceed
- Point of contact person has been identified for each key SP and interface partner component
- Software components are unit and integration tested prior to being interface tested
- All Interface Control Documents (ICD) are considered complete and baselined.
- Orientation/training for the SP Test Team has been conducted

Exit Criteria:

- All interface test scripts have been executed and results have been submitted to the State
- All Severity 1 and 2 defects have been fixed, tested, and closed
- All severity 3 and 4 defects have been identified and a State approved plan exists to resolve them.

9.0 DESCRIPTION OF TESTING ENVIRONMENT

9.1 OVERVIEW

Prior to the start of Interface Testing, the SP will establish QA Environments for each SDU subsystem that will be utilized during the execution of Interface Testing with the Interface Partners. These test environments will be designed to isolate the data and software being exercised during testing in order to allow the SP to tightly control test variables. This section will describe the proposed testing environments for each of the three main components: the Collections Engine, the Disbursements Engine and the CORE Interface Engine.

Each of the three main subsystems will have test environments located at their respective facilities during Interface Testing. Each subsystem will have connectivity via secure FTP to Interface Partners. All inbound files and outbound files will flow through the CORE Interface Engine to all other components, including the Collections Engine, the Disbursement Engine, SWS, CASES, ARS, IDB, CSR and all pertaining Banking institutions. The SP Technical Lead will coordinate with the SP Test Team to configure all communication and database set-up activities, as well as coordination of maintenance and backup activities for the databases as required. Subsystem point of contacts will be used for communication and coordination of these activities.

The following diagram depicts an overview of the QA environments in relation to one another:

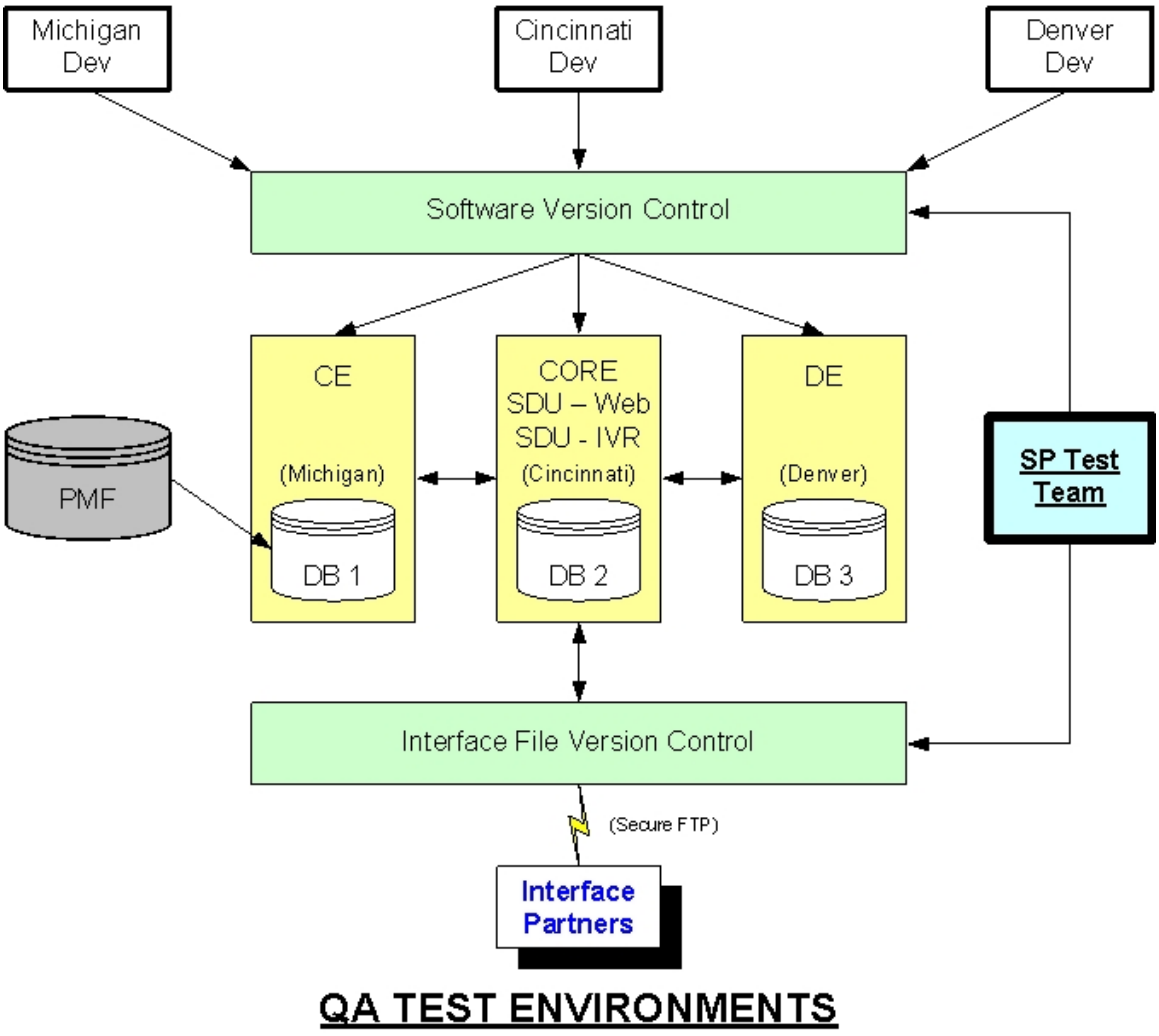


Figure 9-1 QA Test Environments

During Interface Testing, the Interface Partners will send their inbound files using Secure FTP to the SP. The CORE Interface Engine will then take the file, process it, and send it to the appropriate SDU subsystem for processing. Likewise, the outbound files will be sent to the CORE Interface Engine for processing and returned to the appropriate Interface Partner via the secure FTP.

A more detailed description of the test environment for each subsystem can be found in section 9.3.

9.2 Preparation of Test Environments

Each of the facilities that will be utilized to host the test environments for each subsystem, Denver, CO, Plymouth, MI, and Cincinnati, OH, are established development centers that already have in place the infrastructure, protocols and procedures to support the type of test environment needed for Interface Testing. The resources managing these facilities are well versed in providing secure isolated

test environments. The following describes the preparation each group will go through to be ready for Interface Testing:

Collections Engine

- Set up QA server, OPEX scanner, DP500 and LAN environment
- Configure *Visual SourceSafe. Visual SourceSafe* is the software configuration management tool for testing.
- Configure internal system test environment database and application folders
- Configure Interface test environment database and application folders
- Test connectivity to CORE Interface Engine

SDU IVR and SDU External Web

- Set up QA server and LAN environment
- Configure *Visual SourceSafe. Visual SourceSafe* is the software configuration management tool for testing.
- Configure internal system test environment database and application folders
- Configure Interface test environment database and application folders
- Test connectivity to CORE Interface Engine

Disbursements Engine

- Set up QA server and LAN environment
- Configure *Visual SourceSafe. Visual SourceSafe* is the software configuration management tool for testing.
- Configure internal system test environment database and application folders
- Configure Interface test environment database and application folders
- Test connectivity to CORE Interface Engine

9.3 DESCRIPTION OF MULTIPLE ENVIRONMENTS

The following provides a description of the test environments for each of the subsystems being utilized in Interface Testing:

9.3.1 COLLECTIONS ENGINE

The Collections Engine Interface Test environment will be an isolated and controlled environment that is dedicated to SDU Interface Testing. The servers and scanners will be utilized for internal system testing and Interface testing during this timeframe. The development team will not have access to this environment. There will be specific internal code migration procedures, utilizing *Visual SourceSafe* that will be used to promote code to the internal system test environment. The SP Test Team will direct the timing of the releases of this code to the Interface Test environment. The following is diagram of the Collections Engine test environment:

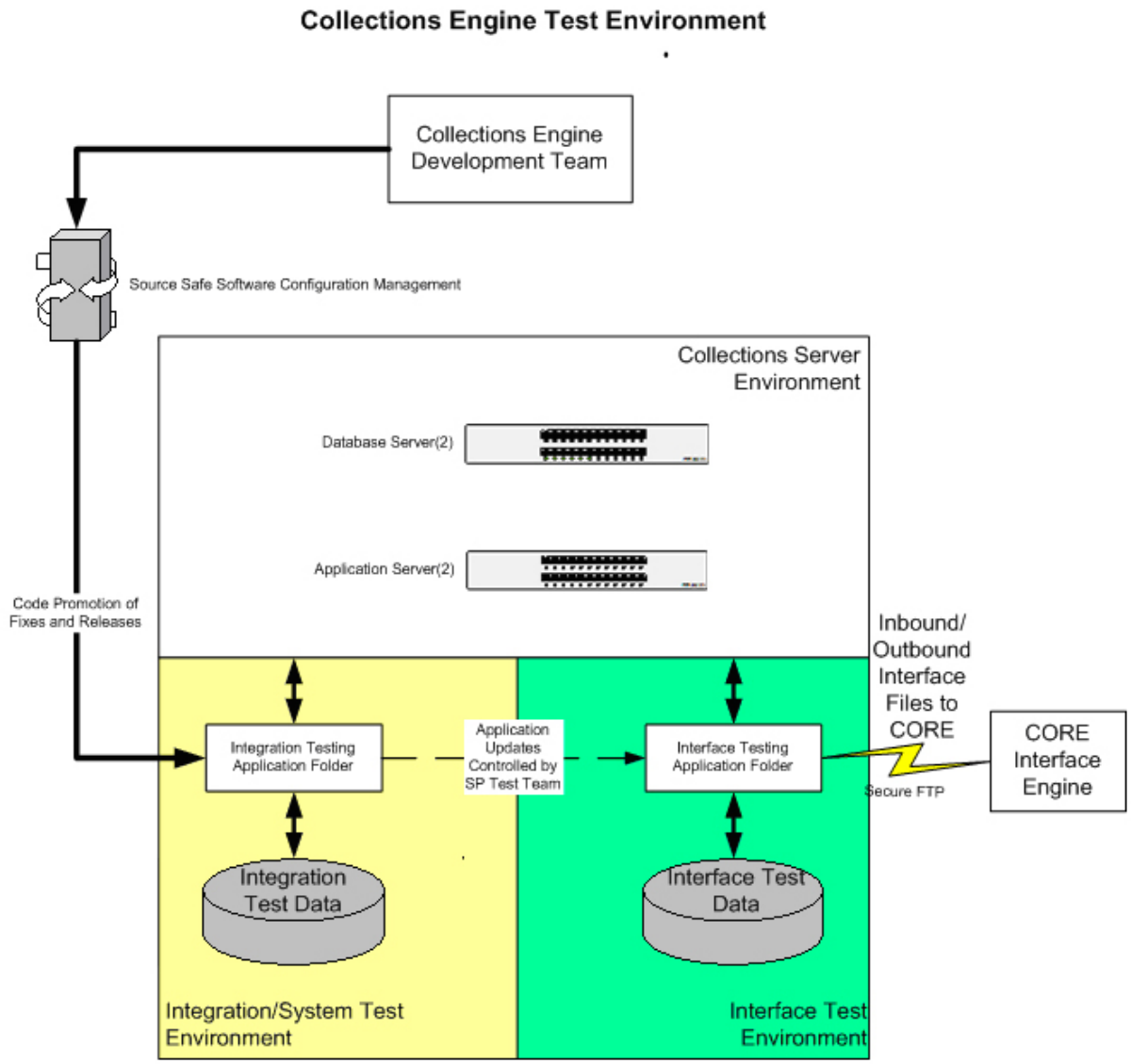


Figure 9-2 Collections Engine Test Environment

As stated above, the interface test files will be sent to the Collections Engine via the CORE Interface Engine. The inbound files will be loaded into the Interface test environment where the SP Test Team will then validate the file in accordance with the appropriate ICD as identified in the associated Interface test script. These files will then be ingested into the Collections Engine. The SP Test Team will validate that the files were ingested successfully and the data was stored successfully. A copy of all inbound files will be stored in a secure location in the Interface test application folder. This will allow the SP Test Team to reprocess the files into the system for generating the outbound files later in the testing cycles.

9.3.2 CORE INTERFACE ENGINE/IVR/WEB ENGINE

The QA environment for the CORE Interface Engine will consist of three separate instances for code repair, internal system testing and Interface Testing. In the CORE Interface Engine test environment the Interface test platform will reside on a

separate physical server platform and network than internal development platform, and internal system testing environment. There is no access to the interface test environment allowed by the development team except for scheduled releases. Releases to the interface test environment will be controlled by the SP Test Team. Below is a diagram of the CORE Interface Engine testing environment:

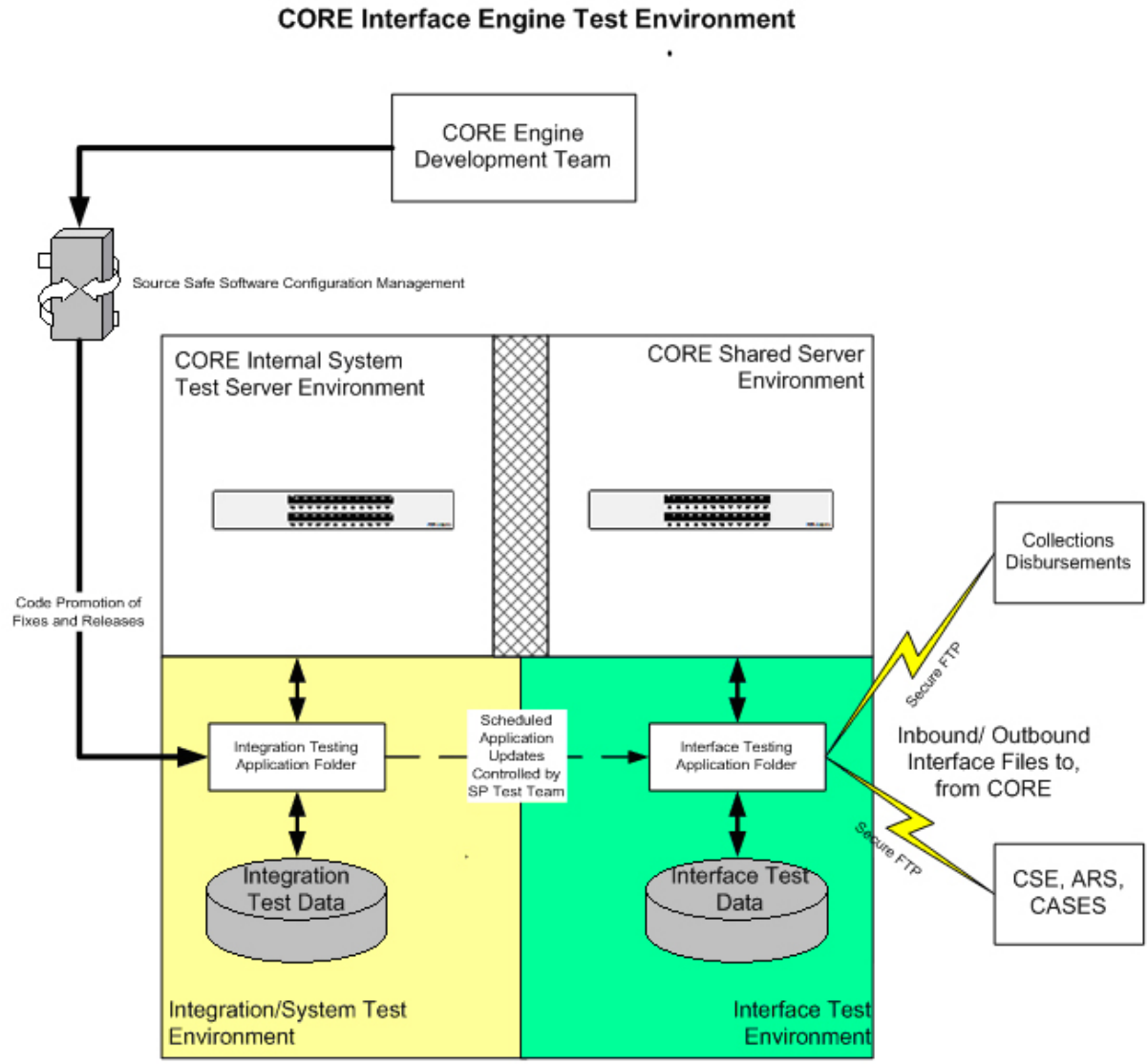


Figure 9-3 CORE Interface Engine Test Environment

9.3.3 DISBURSEMENTS ENGINE

The Disbursement Engine test environment will contain two virtual environments created for testing. An internal system testing environment will be created to allow the SP Test Team to internally test the Disbursement Engine and an interface test environment will be created to support Interface Testing with the Interface Partners.

The system test environment and interface test environment will be isolated. The software and data used for interface testing will be controlled by the SP Test Team. The Disbursements development group will use *Visual SourceSafe* software configuration tools to promote fixes and releases to the test environments. The SP Test Team will manage the promotion of fixes and releases to the interface test platform as needed. The following is a diagram of the Disbursement Engine test environment:

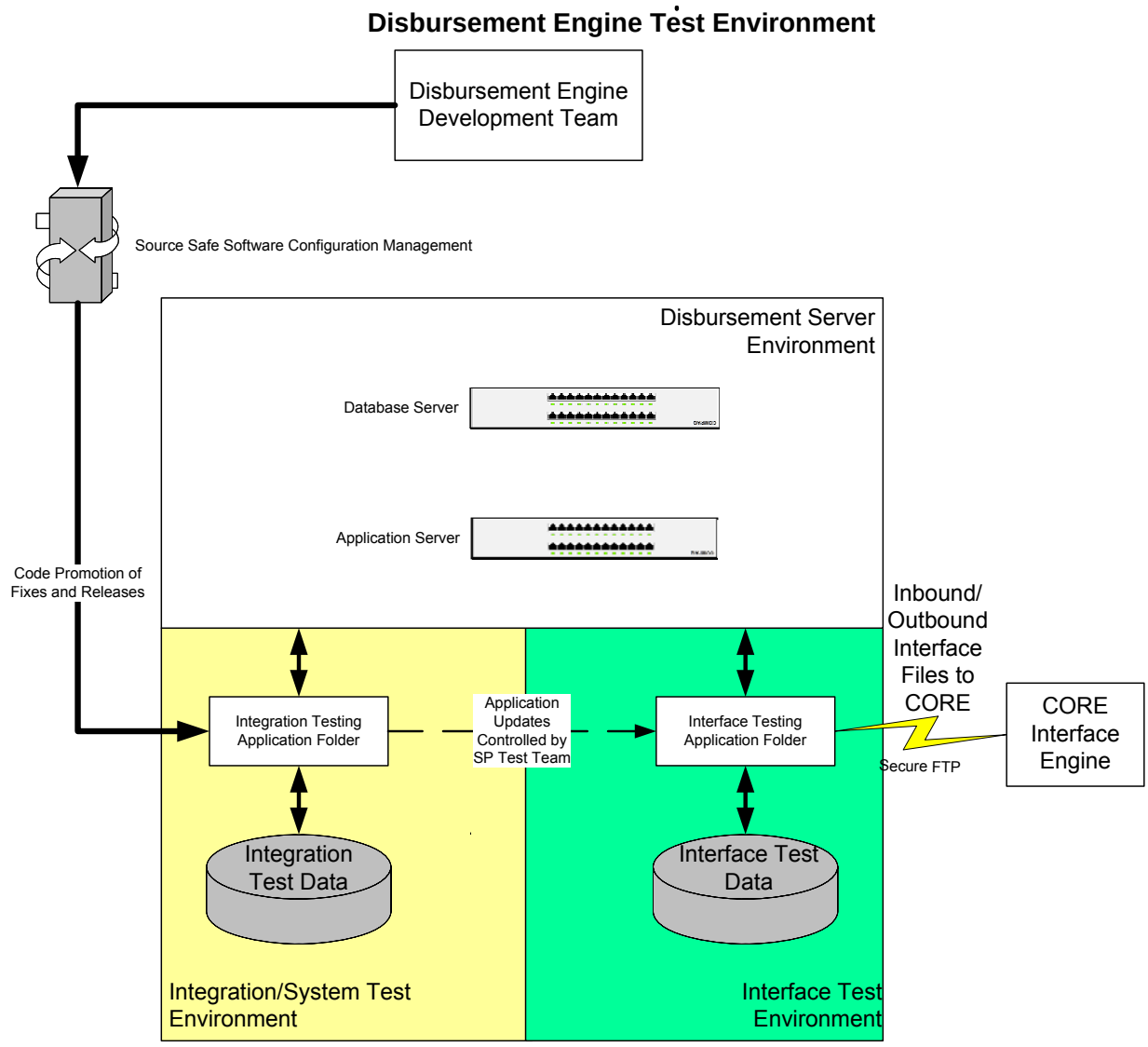


Figure 9-4 Disbursement Engine Test Environment

All printing will be managed out of our SP Print Facility in Chicago, IL. The print facility has an existing test environment that will be utilized for any printing needs during interface testing. The data that is sent to the print facility will only contain depersonalized production data.

9.4 TESTING TOOLS

There are only two testing tools that will be utilized during Interface Testing, the *Test Data* Generator (refer to paragraph 10.4), and *TestTrack Pro*™ (refer to section 12.0).

9.5 OVERVIEW OF HARDWARE AND SOFTWARE

The following Table 9-3 details the SDU Interface Test Environment

CA Interface Test Environment

System	Location Of Environment	Workstation Clients	Servers	Peripherals	WAN	LAN	Security	Technical Support
CORE Interface Engine	Cincinnati, Ohio	SDU Operations testing access via SP WAN Administrative testing access via SP WAN	Dual 3.2 Ghz Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache	Remote printing will be available as needed	Plan A – VPN via Internet Plan B: Extended – Implement DR connectivity early HHSDC to SP WAN (T-1) Unisys to Internet (T-1)	10/100/1000 Standard Ethernet Similar switching to SDU	Physical: Financial Data Center Quality All test participants pre-authorized to access SP/SDU test resources SFTP PGP	Cincinnati Development Cincinnati Networking
Collections Engine	Plymouth, Michigan	(10) Windows clients Testing in Plymouth will be limited to Plymouth LAN only due to security measures.	Server 1 R&L Application Serve, R&L SQL Server, Icapture Image Server, Icapture Aux servers, Icapture Stat SQL server Dual 3.2 GHz Xeon CPU, 2 gig mem, 140	OPEX (1) Unisys NDP 600 (1) Printers (2)	Plan A – VPN via Internet Plan B: Extended – Implement DR connectivity early HHSDC to SP WAN (T-1) Unisys to SP WAN (T-1)	10/100/1000 Standard Ethernet Similar switching to SDU	Physical: Financial Data Center Quality All test participants pre-authorized to access SP/SDU test resources SFTP PGP	Plymouth Development Plymouth Networking

System	Location Of Environment	Workstation Clients	Servers	Peripherals	WAN	LAN	Security	Technical Support
			gig disk, 1 mg L2 Cache Server 2 Image File Server 1.8 ghz CPU, 512 mem, 40 gig HD, 256 Cache SoftCAR Platinum Workstation dual 3.2 GHz cpu, 1 gig mem, 60 gig disk, 512 Cache Server 3 BizTalk Server, Infoimage Exception Server, Archive App Server, Archive SQL server, Archive WEB server Dual 3.2 GHz Xeon CPU, 2					

System	Location Of Environment	Workstation Clients	Servers	Peripherals	WAN	LAN	Security	Technical Support
			gig mem, 140 gig disk, 1 mg L2 Cache					
Disburse-ments Engine	Denver, Colorado	State and LCSA access via SP WAN architecture SDU Operations access via SP WAN Administrative access via SP WAN	App Server Dual 3.2 Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache Database Server Dual 3.2 Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache Web Server Dual 3.2 Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache	Remote printing will be available as needed	SP WAN Only	10/100/1000 Standard Ethernet Similar switching to SDU	Physical: Financial Data Center Quality All test participants pre-authorized to access SP/SDU test resources SFTP PGP Encryption	Cincinnati Development Denver Networking
Check Printing/Outbound Correspon dence Engine	Chicago, Illinois	Test Files will be passed to check and notice printing environment via Internet SFTP –	App Server Dual 3.2 Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache	Remote printing will be available as needed	Internet VPN Only	10/100/1000 Standard Ethernet Similar switching to SDU	Secure FTP All test participants pre-authorized to access SP/SDU test resources SFTP	SP Print facility Cincinnati/Denver Networking

System	Location Of Environment	Workstation Clients	Servers	Peripherals	WAN	LAN	Security	Technical Support
		results will be sent to Sacramento Test team via postal mail					PGP Encryption	
SDU IVR	Cincinnati, Ohio	Standard Public IVR testing, access via internal extensions and external test 800 line Administrative IVR testing access via SP WAN	App Server Dual 3.2 GHz Xeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache Database Server Dual 3.2 ghz zeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache	Remote printing will be available as needed	SP WAN	10/100/1000 Standard Ethernet Similar switching to SDU	Physical: Financial Data Center Quality All test participants pre-authorized to access SP/SDU test resources SFTP PGP Encryption	Cincinnati Development Cincinnati Networking
SDU Web	Cincinnati, Ohio	Standard public Web-based testing access via Internet Administrative Web-based testing access via SP WAN	App/Web Server Dual 3.2 ghz zeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache Database Server	Remote printing will be available as needed	SP WAN Internet	10/100/1000 Standard Ethernet Similar switching to SDU	Physical: Financial Data Center Quality All test participants pre-authorized to access SP/SDU test resources SFTP PGP Encryption	Cincinnati Development Cincinnati Networking

System	Location Of Environment	Workstation Clients	Servers	Peripherals	WAN	LAN	Security	Technical Support
			Dual 3.2 ghz zeon CPU, 2 gig mem, 140 gig disk, 1 mg L2 Cache					

Table 9-3 SDU System/Interface Test Environment

9.6 CONNECTIVITY TESTING

Connectivity testing, as it pertains to Interface Testing will be accomplished through the implementation of the F-Secure SSH® Server and Client (as discussed in section 6.5.3 - File Transfer Protocol (FTP) with interface partners). The files will be transmitted over the internet during Interface Testing. The implementation of F-Secure SSH® will include the provision of installation and process procedures, as well as the F-Secure SSH® Client installation media, to each CCSAS data exchange partner. Once each data exchange partner installs the software, the SP F-Secure SSH® administrator will work with each partner to test and validate that the system and procedures work according to the provided documentation. Given that this connectivity infrastructure will only be utilized during the Interface Testing Phase from 4/4/05 to 6/15/05, it does not represent the connectivity architecture that will be in place once the SDU facility is occupied and HHSAD WAN connectivity is in place.

Connectivity Testing as it pertains to the production facility/environment will be performed after 6/15/2005. In addition to testing wide area network connectivity as whole, the SP will facilitate the graceful transition of interface file exchanges from the F-Secure SSH® model to the actual production model.

9.7 LOCATION OF TESTING

The SP Interface Testing will occur at the following locations:

- Sacramento, California (SP Test Team)
- Denver, Colorado
- Plymouth, Michigan
- Chicago, IL
- Cincinnati, Ohio

Table 9-3 details the SDU subsystem and location of testing. The Sacramento location is the site of the SP Test Team and the *Test Data Generator*.

10.0 DESCRIPTION OF TEST PREPARATION ACTIVITIES

10.1 APPROACH TO OBTAINING, PREPARING, MAINTAINING AND CONTROLLING TEST DATA

A critical component to successful testing is the process of identifying, collecting and managing appropriate test data throughout the lifecycle of the implementation. The SP Test Team will utilize data obtained from SWS through the Participant Match File and use the *Test Data Generator* tool to store, create and maintain all of the test data for Version 1 testing. The following diagram, Figure 10-1, provides an overview of this process.

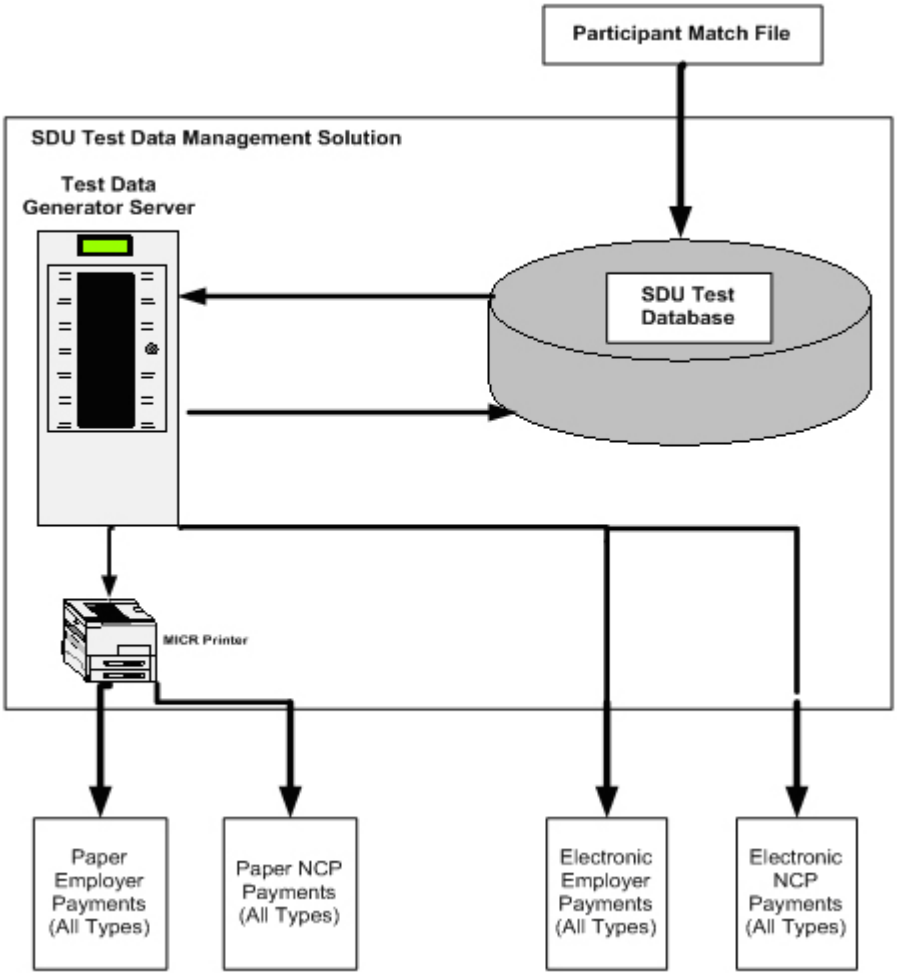


Figure 10-1 Overview of Test Preparation Activities

10.2 PARTICIPANT MATCH FILE

The SP Test Team will generate all test data for interface testing from the Participant Match File provided by the BP. The SP will receive the Participant Match File by secure FTP during Interface Testing. The BP interface partner will provide a database extract from the SWS system to generate the data elements required. The

SP will receive the database extract and execute SQL stored procedures to create the Participant Match File required by the Collections Engine. The Participant Match File will contain participant data elements, for example: Participant Name, Social Security Number, Court Case Number, Participant Number, and Case Number.

By doing this, all test data produced by the SDU system will correspond to the test data being produced out of SWS. The collections files will contain payments that SWS can recognize and process.

10.3 SDU TEST DATABASE

The SP Test Team will utilize a SQL relational database to store all data from the Participant Match File, as well as any employer data that can be obtained from SWS. The database will allow the SDU to have a single controlled repository for all test data that can be managed and maintained throughout all test activities. The database will be housed at the interim project facility until the permanent SDU facility becomes available. The SP Test Manager and Test Lead will control all output from the test database.

10.4 TEST DATA GENERATOR

A key component to the SDU test data management solution is the *Test Data Generator*. This tool will access the test data stored in the SDU test database to produce test data that will be used to either initiate or conduct all the Interface testing. The *Test Data Generator* is designed to create child support payments including:

- Employer Lists
- Employer Single Payments
- Employer EFT Payments
- NCP payments
- NCP EFT Payments
- Scannable Employer and NCP Payments
- Interstate Payments
- CP
- Other agencies

In addition to creating payment transactions, the *Test Data Generator* can produce exception payment transactions. Creating exception payments will allow the SP Test Team to validate exception conditions systematically. The tool can be configured to create various exceptions for testing including, but not limited to:

- Unbalanced Transactions
- Mismatched Transactions
- Foreign Transactions
- Unidentified Payments

The *Test Data Generator* prints all test payments and clearly marks the payments as test documents, including a void stamp on any checks that are printed.

In addition, the tool has the ability to create and save test payment transactions. All test data that is created can be saved and regenerated on demand. This capability will allow the SP Test Team to tightly control test data to a particular test activity and control the inputs into the test. This level of control will allow the SP Test Team to simultaneously conduct multiple tests and isolate the test data appropriately. For example, the test data generated to conduct Interface testing can be easily separated from the test data used to conduct internal System testing. Lastly, this functionality will also allow the SP Test Team to effectively conduct regression testing. Test data can be regenerated automatically in order to regression test any scenario quickly and accurately.

11.0 DESCRIPTION OF TEST MATERIALS

11.1 TEST PLANNING MEETINGS AND WORKSHOPS

The SP Test Team conducted several internal test planning meetings, as well as meetings with the State and interface partners during the initial test planning.

11.2 DEVELOPMENT OF TEST SCENARIOS

During the test planning phase, the test scenarios were developed. The test scenarios focused on specific functional areas of the system and provided detailed information about the situation to be tested as well as step-by-step instructions to guide a tester through the execution of the test scenario. Test scenarios were developed to cover the most common situations that users encounter while performing their duties in a real life situation and covered all requirements identified from the RFP, SOWs and requirements-gathering sessions with the State.

11.3 DEVELOPMENT OF TEST SCRIPTS

Once the high level test scenarios were identified, the individual test scripts were designed to help ensure a complete test of each scenario. The number of scripts required to test a scenario vary depending on its complexity. Test scripts are written to encompass either a single situation or incorporate multiple situations. By carefully following each test script and verifying specific expected results, the SP Test Team will be able to certify that the system requirements have been successfully met. The test scenarios and test scripts are controlled, managed and tracked in the SP testing database. The inputs to the interface test scripts included the RTM, IID, ICDs, and discussions with the developers. The scripts were reviewed by the developers and Test Support Team prior to assigning a completion status within the project plan. These Test Scripts will also be made available to the state for review. The internal system testing will rely on the execution of the inbound interface test scripts. This data will be used throughout end to end system testing, and ultimately the system tests will use the outbound test scripts to generate the outbound interface files.

The SP Test Team is responsible to make any updates that are required to the RTM as a result of requirements being added, modified, or deleted from the change control process. After this information comes into the team, updates will be made to any scripts that are affected by the changes to the requirements.

The following diagram, Figure 11-1 shows the flow from test meetings to test plans and to test scripts.

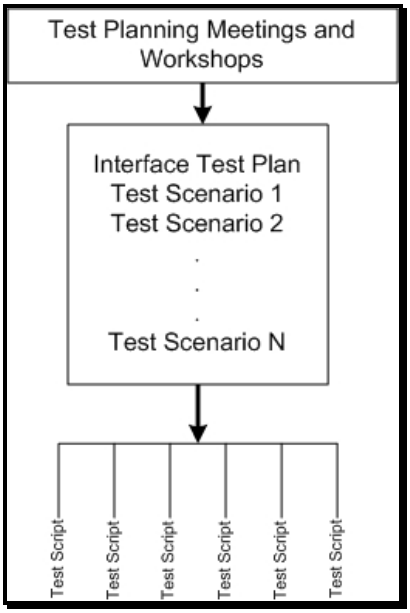


Figure 11-1 Test Planning

11.4 REQUIREMENTS TRACEABILITY MATRIX

In order to verify that sufficient test scenarios have been created to thoroughly test all of the system requirements, the SP testing database includes a Requirements Traceability Matrix (RTM) that maps each test script to the corresponding requirement that is being tested. The Requirements Traceability Matrix includes RFP requirements, SOW requirements, and a compilation of requirements that were identified by the project outside of the RFP and proposal during meetings with interface partners to develop the IIDs.

The SP Test Manager coordinated the effort to receive and compile the completed RTM. Once the RTM was compiled, it was reviewed and signed off by the Solution Configuration Team. The SP Test Manager requested and ensured that the Solution Configuration Team completed the SDU Requirements Traceability Matrix Signoff form. After receiving sign-off, the RTM was considered baselined and any changes to the RTM will follow the internal SP Change Management process. A copy of the RTM was sent to the State and can be sent to any partners upon request. This process is documented in the SP internal Change Control document located in the SP eRoom at the below URL and can be sent upon request.

https://eroom.govconnect.com/eRoom/external/CACSESDUPre-Contract/0_3d034

In order to enable repeatability of interface testing efforts, the interface test scenarios are linked to the requirements in an Excel spreadsheet. The interface test scripts are tracked in the SP test database. As interface test scenarios and test scripts are completed successfully, the SP Test Team will track test coverage as it relates to the interface requirements.

12.0 RECORDING AND MONITORING DEFECTS

12.1 APPROACH

In order to properly manage defects across the SDU subsystems the SP Test Team will utilize at a minimum, the following elements to track each defect within our *TestTrack Pro*™ database:

- Defect Title
- Defect Detail Description
- Defect History
- Severity
- Priority
- Found By
- Date Found
- Assigned By
- Assigned Date
- Test Phase
- Test Scenario
- Test Script
- Software Release Version
- Defect Workflow as depicted in Figure 12-1

TestTrack Pro™ supports a comprehensive workflow structure that will be customized to support SDU Interface testing. The workflow that the SP Test Team plans to utilize for all phases of testing is depicted in the following diagram, Figure 12-1.

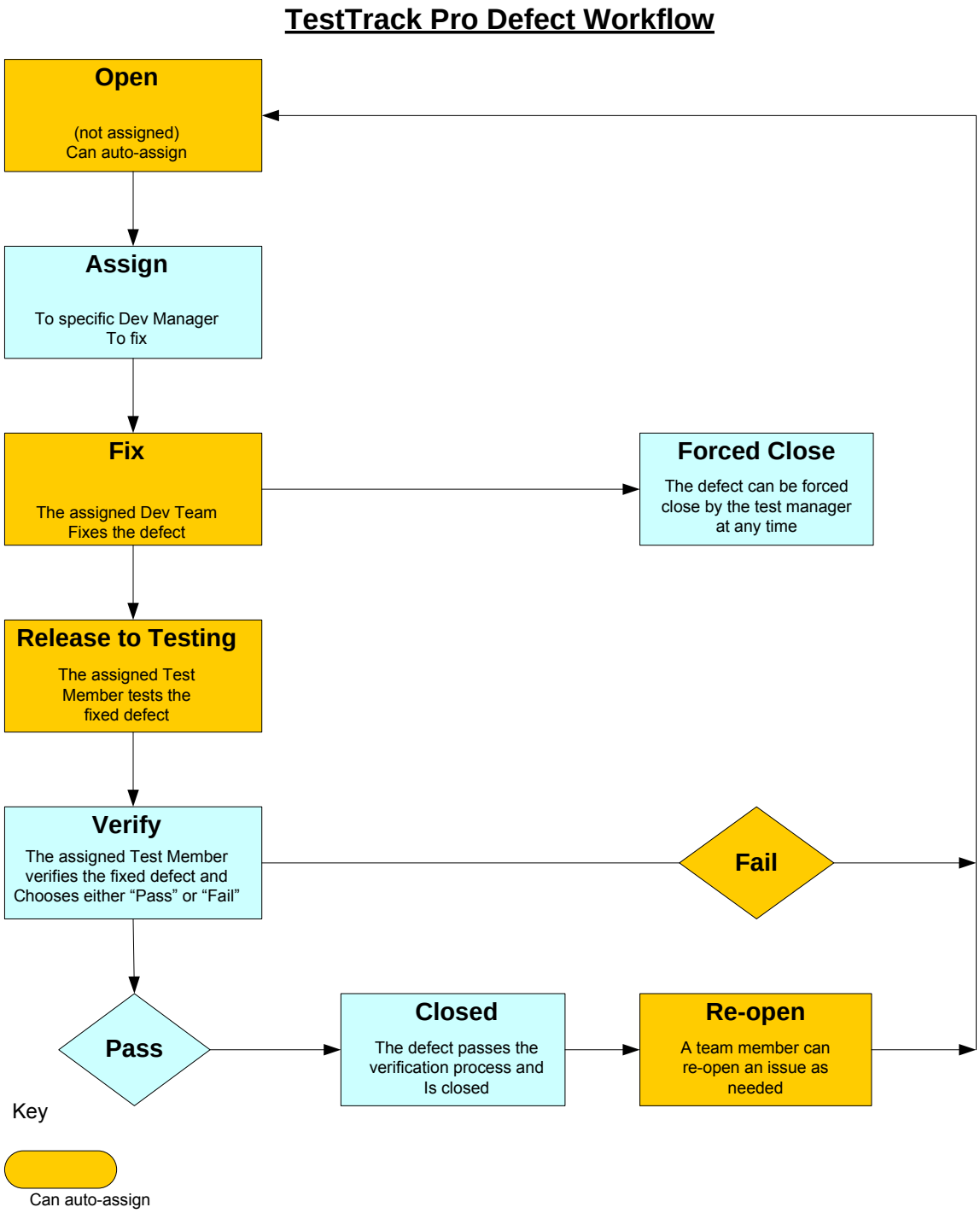


Figure 12-1 TestTrack Pro Defect Workflow for SDU subsystems

During the interface testing, analysts, managers, testers and developers will work in teams to run test scripts, identify defects and resolve these defects in a controlled QA environment. This controlled QA environment will include structured source code management, daily defect reviews, secured access to the centralized *TestTrack Pro*™ defect tracking and management system, and most importantly, weekly interface partner reviews of test status by CASDU subsystem.

12.1.1 DEFECT DEFINITION

The SP Test Team will track defect status in accordance with the defect tracking definitions used by the BP. The following sections 12.1.1.1 to 12.1.1.2 are taken from IM 001 with the direction from the State to utilize the Problem Prioritization identified in the *Problem Resolution Management Plan* (*Section 2.4.3.3, pps. 30-32, CDL TM 010*, dated March 29, 2004).

It is acknowledged that the State reserves the right to determine severity levels for defects.

12.1.1.1 PROBLEM PRIORITIZATION

1. Determine Impact. Impact is an estimate of the measure of users, systems or services that are disrupted by the identified problem. The Daily Defect Review Meetings will discuss the impact based on the description provided by the initiator and the scale detailed in the following table.

Value	Impact
1	• System-wide impact affecting all users or testers on the application in a particular environment, regardless of function
2	• System-wide impact affecting all users or testers of a function on the application in a particular environment
3	• Impacts users across multiple counties or throughout a large county in production, or impacts most testers across all of the teams
4	• Impacts multiple users within a particular county in production, or impacts multiple testers on a team
5	• Impacts a single user or several users within a small group in production, or impacts one tester in an environment

Table 12-1 Impact Definitions

2. Determine Severity. Severity measures how quickly the problem must be resolved to minimize the adverse impact to the project or users. The Daily Defect Review Meetings will assign a numerical value for Severity, based on the description provided by the initiator and the scale provided below:

Value	Severity
1	• Production: Prevents the accomplishment of an essential function • Production: Critical, Jeopardizes safety, security or other requirement designated.
2	• Production: Adversely affects the accomplishment of an essential function and no work-around solution is known • Production: Adversely affects technical, cost or schedule risks to the project or to life cycle support of the system, and no work-around solution is known. • Testing: Prevents accomplishment of essential function or test.

Value	Severity
3	• Adversely affects the accomplishment of an essential function but a work-around solution is known
	• Adversely affects technical, cost or schedule risks to the project or to life cycle support of the system, but a work-around solution is known. • Testing: Adversely affects the accomplishment of an essential function and no work-around solution is known • Testing: Adversely affects technical, cost, or schedule risks to testing, and no work-around solution is known.
4	• Results in user/operator inconvenience or annoyance but does not affect a required operation or mission essential function • Results in inconvenience or annoyance for development and maintenance personnel, but does not prevent the accomplishment of those responsibilities
5	• Any other effect

Table 12-2 Severity Definitions

3. Calculate a value for *Priority* from the Impact and Severity values using the matrix shown below in Figure 12-2. Priorities are established using a numerical scale ranging from 9 (lowest priority) to 1 (reserved for Emergency Fixes). The initial weighting of the priority scale provides equal weighting for both impact and severity.

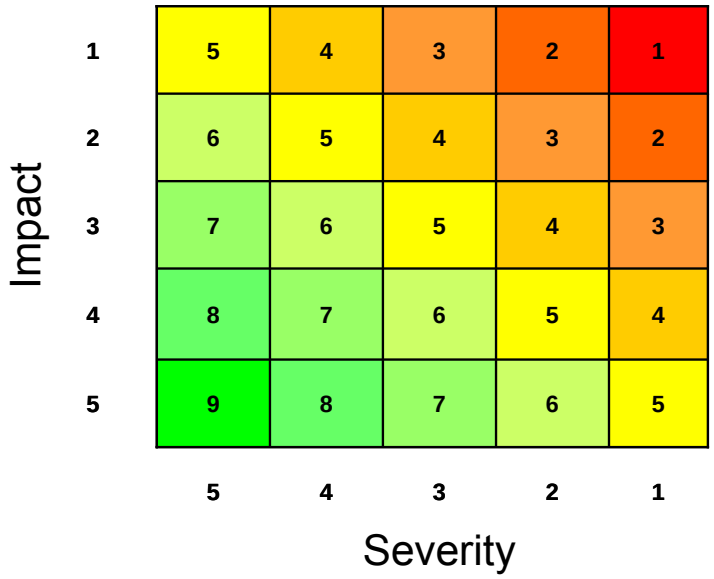


Figure 12-2 Problem Prioritization

This matrix provides the team with a consistent, objective way to set a numerical value for Priority based on the breadth of the problem (Impact) and the urgency of the problem (Severity).

12.1.1.2 LEGEND – DEFECT STATUS

The following defect statuses are used within the defect tracking tool:

- **Open** - Defect identified and recorded
- **Assigned** - Open defect assigned to developer for resolution
- **Fix** - Defect corrected by developer, but not yet included in a software release
- **Forced Close** – A defect that was opened but is unable to be reproduced. The SP Test Manager will have access to Forced Close if the defect is unable to be reproduced or if a duplicate defect is entered.
- **Release to Testing** – Open defect that has been fixed and released to testing for verification
- **Verify** – The defect that is assigned to the test team to verify the defect
- **Closed** - Defect corrected, included in a software release, and correction verified

12.1.2 SOFTWARE CONFIGURATION CONTROL AND PROMOTION

The SP Test Team will incorporate standard industry tools and practices for software configuration control and code promotion during all testing activities in Version 1 as described in Section 9. Each subsystem component will follow a strict protocol for the release, testing and promotion of software to resolve defects identified during testing. The following diagram, Figure 12-3, is a high level diagram of the process that will be utilized to address defects and release fixes.

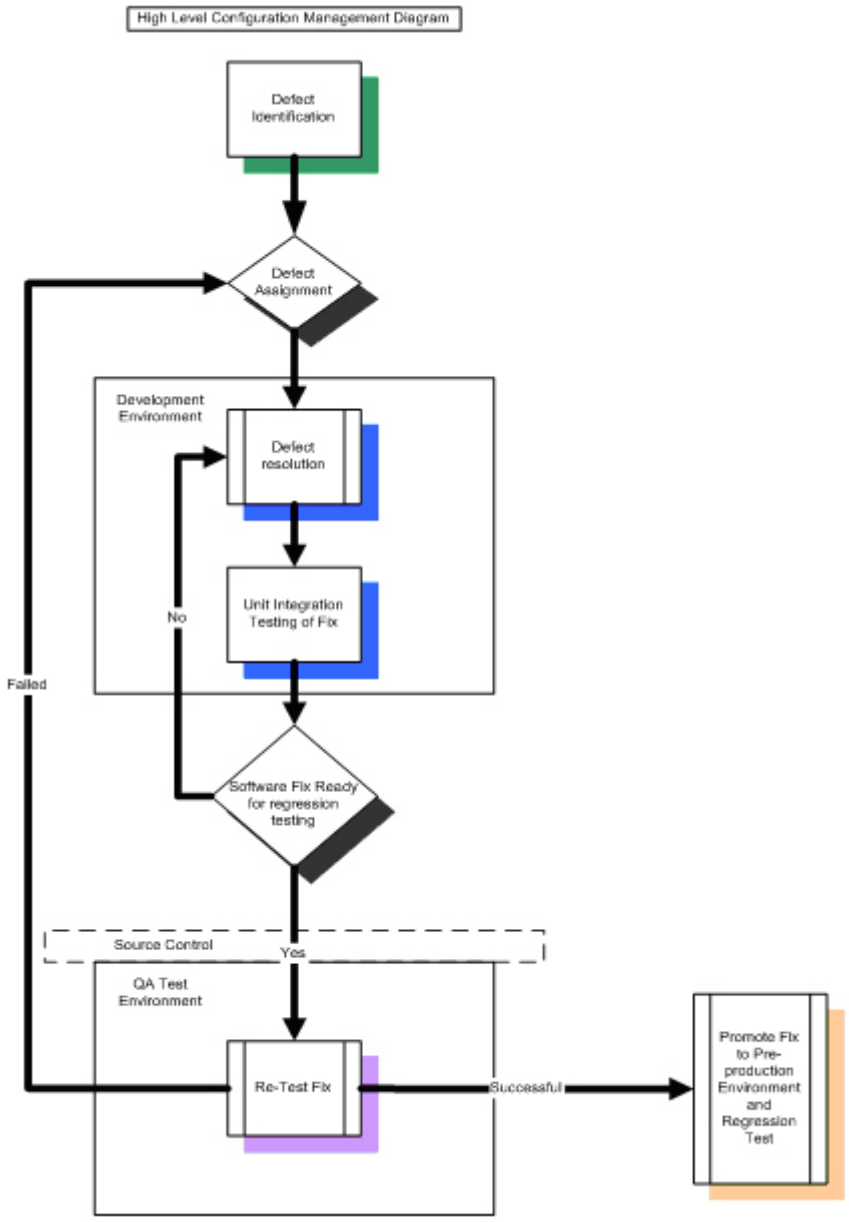


Figure 12-3 Software Configuration Control

12.1.3 DEFECTS AFFECTING THE INTERFACE PARTNERS

Defects identified by the SP Test Team that need to be addressed by the interface partners will be tracked in *TestTrack Pro™.* The SP Test Team will not utilize the ClearQuest or TestDirector tools. The SP Test Team will provide the interface partners with the defect reports for defects assigned to them. Additionally, we will receive the defects from Interface Partners in either a report, spreadsheet or an email.

If a problem is identified by an interface partner, and it is a problem with the SDU solution:

- The Interface Partner submits the defect to the SP Test Team via e-mail, and a defect will be created in *TestTrack Pro*™.
- The SP Point of Contact person will follow up with the Interface Partner via e-mail or phone confirming the receipt of defect.
- The defect will be tracked along with tracking the defects from the SDU system.
- Upon resolution, the SP Test Team would notify the originator that the defect was closed via email.

If the problem is identified by the SP, and it is a problem with an interface partner solution:

- The SP Test Team logs the defect as Open.
- *TestTrack Pro*™ issues an automated email to the interface partner contact to notify them that a defect was found.
- The SP Test Team will be notified by the Interface Partner when the defect is corrected and the status will be updated from *Open* to *Release to Testing.*
- The SP Test Team performs a retest and will mark the defect as *Closed* or re-open the defect by selecting *Open*.

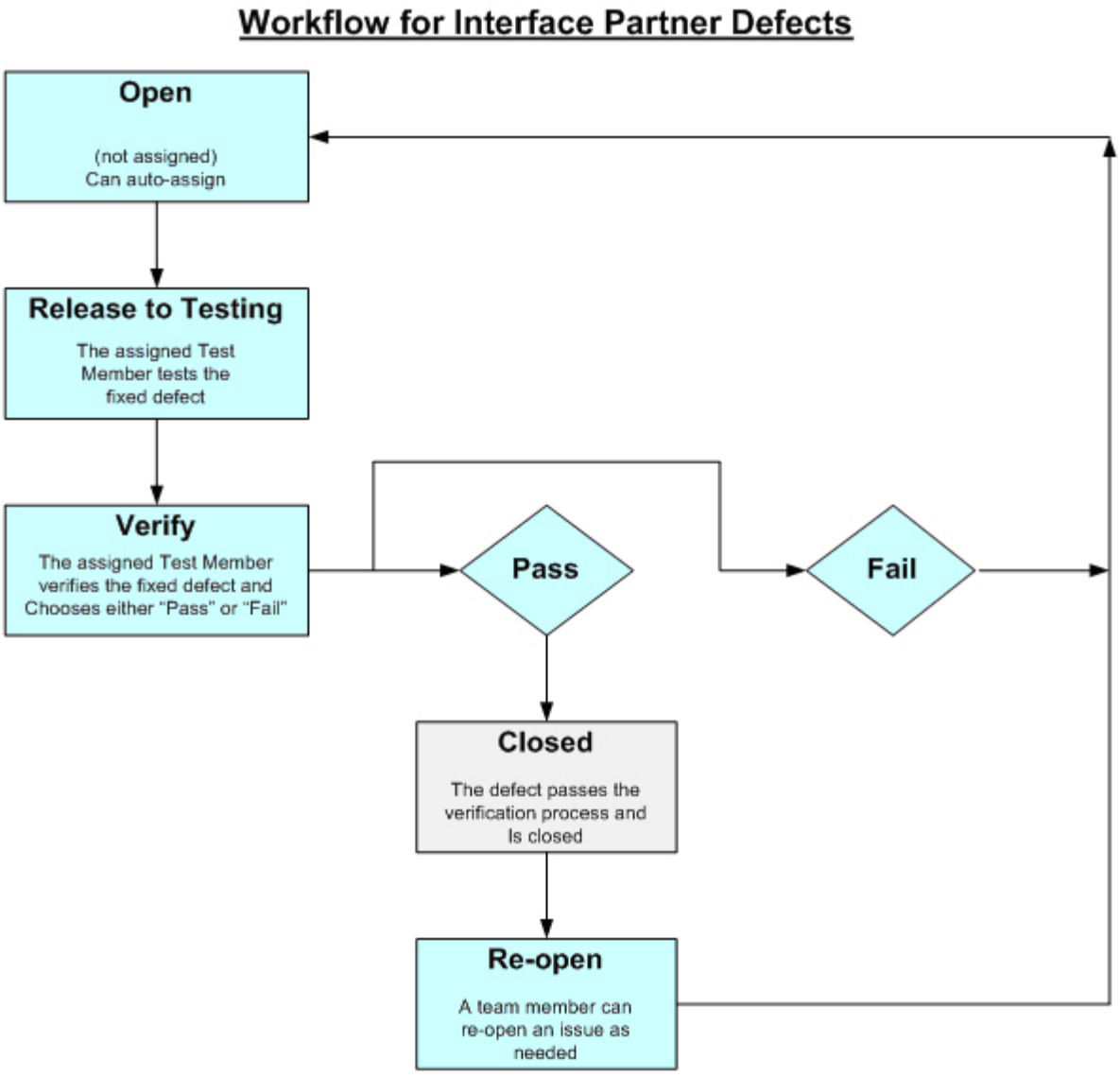


Figure 12-4 TestTrack Pro Defect Workflow for Interface Partners

12.1.4 Corrective Action Process

Each development organization will be responsible for implementing an internal corrective action process. When the problem is fixed the SP Test Lead (or designated representative) will be provided with a build/release transmittal that includes:

- A list of defects that were fixed in the build
- A brief assessment as to what caused the problem
- The software modules affected
- Installation packages of the new modules labeled with unique version numbers and any changes to the installation or usage instructions

- Additional verifiable information. For example: version number, date/time, and file size, must be attached with each changed item for verification

System/database administration personnel will be responsible for installation of all system configuration control items. All changes to the system configuration must be coordinated through the SP Test Lead and performed by assigned administration personnel.

13.0 DESCRIPTION OF TEST EXECUTION

13.1 EXECUTION OF TEST SCRIPTS

Each tester will be assigned to specific test scripts for execution. Prior to executing the test script, testers will review the design documentation and requirements to become familiar with the functionality to be tested.

After each step is completed, actual results will be documented on a hard copy of the test script. The tester will then transfer those results to the test and defect tracking system using the expected results to determine whether all steps in a test script were successful. If a certain step within a test script fails to meet the expected results, the step will be deemed *Fail* and a defect will be recorded in the test and defect tracking system. During execution, any supporting artifacts and output documents will be produced and forwarded to the appropriate interface partner. If a particular test step is in progress but not complete, the test step will be left blank.

13.2 RECORDING RESULTS IN THE TEST AND DEFECT TRACKING SYSTEM

The SP Test Team will use *TestTrack Pro*™ during implementation to provide all of the tools necessary to automate the recording, evaluation and resolution of defects.

13.3 RETESTING AND RESOLVING DEFECTS

The SP tester will compare the expected results detailed in each step of a test script with the actual results received during testing. If a certain step within a test script fails to meet the expected results, the step will be deemed *Fail* and a defect will be recorded in *TestTrack Pro™*. As defects are identified and resolved, software releases will be incorporated to address the defects. The SP Test Team will retest the defects and regression test the releases. The test script will be re-executed for retesting. The SP tester will document the retest results on hard copy of the test script as well as transferring the results to the SP testing database contained in *TestTrack Pro™*. The SP testing database will track the number of test scripts that required retesting. Additionally, the SP Test Team will update the defect status in *TestTrack Pro*™ as either Closed or Open depending on the retest results. Comments can be added at any time to the defect. Additionally, the SP tester will utilize the comments field to enter the test results as well.

13.4 VALIDATING COVERAGE OF TESTING

The SP Test Team's testing approach includes a combination of techniques to validate test coverage and completeness. The test scripts that are developed will be housed in the test and defect tracking tool. The test scripts will map back to requirements in order to validate test coverage. Also, test plans will be developed with input from the State and appropriate interface partners, as well as any other Subject Matter Experts (SMEs), in order to help ensure coverage and completeness of testing.

13.5 MAKING TEST RESULTS AVAILABLE TO INTERFACE PARTNERS

Test results will be recorded during each detailed test. Upon the completion of each Interface Test, the SP Test Team will record the Pass/Fail test results in *TestTrack Pro*™. These Pass/Fail results can be made available to each interface partner following each interface test.

Upon the completion of Interface Testing, the SP Test Team will conduct a review of all recorded test results in *TestTrack Pro*™. The SP Test Team will make all test results available in the Interface Test Report (IM 009) for each of the interface partners.

14.0 REGRESSION TESTING

14.1 OVERVIEW

Regression testing includes any test activities conducted to confirm the integrity of the system after code has been changed to resolve open defects or if a new release of software has been introduced. The SP Test Team will conduct regression testing during Interface testing in the event that the software environment has been modified by a fix, a new release or any other maintenance activities. As part of regression testing, we will also be retesting fixes. The main goal is to help ensure that modifications have not created defects in areas not obviously touched by the change.

The *Test Data Generator* will allow the SP Test Team to effectively retest specific/restricted test scenarios and scripts through the use of specific test data sets that focus on the appropriate workflows. Essentially, the *Test Data Generator* can create and save test payment transactions that are designed to test a certain scenario or set of scripts. The saved test payment transactions can also be regenerated automatically for the purpose of regression testing any scenario quickly and accurately. If a test script fails and a new release is made to address the defects, the SP Test Team can re-create the exact conditions that caused the test script to fail and regression test the software to confirm the defects are resolved.

In addition to utilizing the *Test Data Generator* to assist in regression testing, specialized regression test scenarios will be created. These specialized scenarios link interrelated test scripts to each other for the purpose of regression testing specific workflows that rely on each other to function properly.

For defects found relating to Interface Partners' systems, the SP Test Team will retest the defect after notification is given from the Interface partner that the defect is resolved. The SP External Test Support Manager will coordinate the test schedule to accommodate the additional testing.

15.0 SECURITY AND PRIVACY PROTECTION CONSIDERATIONS

15.1 DATA SECURITY WITHIN THE ENVIRONMENT

Data transmission security in the Child Support industry is considered to be equally significant and imperative as it would be for any other finance based industry. Given this fact, interface transmission security and information system security in general are paramount to the success or failure of the data transmission process as a whole. Driven by our knowledge, experience and the SDU RFP SOW requirements, the SP utilizes several tools and processes to ensure that our data transmission and information system architectures are secure.

Interface Transmission Security – During Interface Testing, the SP will utilize cryptography tools to encrypt transmissions that do not take place completely within the HHSDC network. Prior to SDU site readiness, the SP will provide a Secure Shell (SSH) server based on industry leading F-Secure® SSH technology.

F-Secure® SSH is a file encryption and transmission application based on the SSH protocol that protects critical servers, data transfers, and corporate applications from Internet spies, hackers, and other known security threats. In other words, it encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. F-Secure SSH supports a broad range of cryptographically strong integrity checks, namely SHA-1 and MD5, to repel insertion attacks. In addition, SSH2 adds a number of new features to provide a stronger, more comprehensive product. These features include:

- Encryption ciphers, such as 3DES and AES.
- The use of sound cryptographic Message Authentication Code (MAC) algorithms for integrity checking.
- Support for public key certificates

From a system configuration perspective, F-Secure SSH has two components:

1 - An SSH client which can run on a Windows PC or UNIX workstation. The F-Secure SSH client includes four integrated tools:

- F-Secure SSH Terminal, which secures remote logins over unknown or untrusted networks.
- F-Secure SSH File Transfer, which safely delivers confidential data to authorized users.
- F-Secure SSH Tunnel, which creates a secure transmission link for TCP-based applications.
- F-Secure Authentication Agent, which creates and stores private keys used in the SSH public key authentication method

2 - An SSH server on the system being accessed. The F-Secure SSH server authenticates and encrypts traffic at the server to:

- Safeguard terminal connections.
- Forward Internet protocols, including X11, POP3, SMTP, and HTTP.
- Protect file transfers.

(Please see Appendix D to review the F-Secure SSH Data Sheet, or visit *http://www.wrq.com/products/reflection/ssh/* for a more in-depth description of this product.)

During Interface Testing, the SP will use F-Secure SSH to exchange data with each CCSAS data exchange partner, as well as internally to our Collections and Disbursements engines located in Michigan and Colorado. The F-Secure SSH Server will reside in our Cincinnati, OH Data Center and be accessible via the Internet. F-Secure Clients have been loaned to the CCSAS data exchange partners as needed.

General System Security – For Interface Testing, the SP will be utilizing production data derived from ARS and CASES in the SDU test environment. As it pertains to data transmissions and data management in general, the SP is prepared and equipped to support all security related SOW requirements. The details of all system level security policies and procedures will be included in SDU CDL OM 006 – SDU Security Plan, but given that IM 008 is being delivered earlier than the OM 006, we are addressing each pertaining SOW requirement as it relates to data transmission and supporting system security in the following table:

Req #	Detail	SP Fulfillment
OM 4.9	The SP shall implement mechanisms to maintain an audit trail for all transactions.	The CIE is equipped to maintain an audit trail of all inbound and outbound file transmissions, as well as on a record-level basis. All records within a transmission file are imported into a specified data base table, or a set of database tables for such transmissions as the Participant Match File. Audit trails will be recorded and stored to disk for the duration of Interface Testing for all inbound and outbound transmissions.

Req #	Detail	SP Fulfillment
OM 4.10	The SP shall record supervisor override and bypass events in the Override and Bypass Log. The Override and Bypass Log shall contain sufficient information to determine who authorized the change, the date/time of the change, and reason for the change. The Override and Bypass Log shall be available for inspection by the State.	The SP does not plan to utilize the concept of supervisor overrides or bypass events as it pertains to our data transmission and management efforts. The CIE will only accept or reject transmissions based on predefined business rules. Any failures will be worked out with the corresponding data exchange partner, and remedies to resolve failures will be addressed by the originating system and retransmitted.
OM 4.11	The SP shall establish system security mechanisms such that system, terminal, and password identifications [are] controlled, randomly selected, and uniquely identify the system user.	All SP that drive or interact with data transmission activities will all utilize standard authentication mechanisms such that system, terminal and password identifications are controlled, randomly selected and uniquely identify the system user. During System and Interface testing (4/4/05 to 6/15/05), the SP will utilize similar system security mechanisms to control passwords using F-Secure.
OM 4.12	The SP shall establish system security mechanisms such that password security must extend to the functional screen level and limit the user's capability to view and/or update those screens.	All SP that drive or interact with data transmission activities will all utilize system security mechanisms such that password security must extend to the functional screen level and limit the user's capability to view and/or update those screens. From an interface transmission perspective, only CIE, CE and DE System Administrators will be able to view and/or update data transmission related screens. All operations personnel who handle actual collections and disbursements payment

Req #	Detail	SP Fulfillment
		processing activities will be prevented from using the data transmission and import/export functions of each pertaining subsystem
OM 4.13	The SP shall establish system security mechanisms such that the system must automatically require the system user to change passwords periodically.	All subsystems that drive or interact with data transmission activities will include system functions for forcing all users to change passwords periodically.
OM 4.14	The SP shall provide security levels for access to records and files and utilize automatic sign-off techniques.	All SP subsystems that drive or interact with data transmission activities integrate user and group based security levels for access to records and files and utilize automatic sign-off techniques
OM 4.15	The SP shall develop and implement procedures for system and terminal user identification assignment, maintenance, and cancellation of access rights. Delegation and maintenance of the password system must be limited to a select number of people; and a mechanism must be in place to quickly notify those responsible when there are personnel changes.	As it pertains to data transmission activities, the SP will develop procedures for system and terminal user identification assignment, maintenance, and cancellation of access rights. In addition, only a select group of System Administrators will have the ability to delegate and maintain password for the various subsystems. Human Resource procedures will also be put in place when personnel changes are made that could effect data transmission and data management across all subsystems.
OM 4.16	The SP shall implement security measures to detect, report, and lock unauthorized attempts to gain access to system software and data.	Intrusion detection systems, and other automated analysis techniques will be used to detect, report and lock unauthorized attempts to gain access to data transmission files and any associated subsystem. The SP will work closely with its data exchange partners to ensure that

Req #	Detail	SP Fulfillment
		both parties involved in each transmission are synchronized as it pertains to security.
OM 4.17	The SP shall ensure that IRS data acquired by the system must be protected from unauthorized inquiries and must [keep IRS data] in a separate data file if necessary to ensure its security.	During CCSAS Version 1, IRS data will be transmitted from the IDB to SDU and SDU to SWS. The CIE, CE and F-Secure will all utilize specific user/group authentication and independent user interfaces to ensure that IRS data is kept thoroughly segregated and confidential.
OM 4.18	The SP shall maintain an auditable record of all changes to critical records and/or data fields including identification of the responsible system user and date/time of the change.	All databases and data transmission subsystems utilized by the SP include auditable records of all changes to critical records and/or data fields including identification of the responsible system user and date/time of the change. During Interface Testing, the SP test team will be changing records to invoke business rules. This will not be audited during Interface Testing.
OM 4.19	The SP shall routinely [monitor] the access to use of the automated system.	The SP will create IT policies and procedures, and utilize industry standard tools to routinely monitor access and use of all of its automated systems.
OM 4.20	The SP shall facilitate that an audit trail of all operating system actions must be maintained either on the automatic console log or on the computer system's job accounting file.	All SP subsystems are Windows based and all operating system logging functions will be activated to maintain a detailed audit log of OS activities.
OM 4.21	The SP shall limit access to system utility programs to necessary individuals with specific designation.	Only a select group of System Administrators will have the ability to access and utilize system utility programs that are associated with data transmission and data management functions

Req #	Detail	SP Fulfillment
OM 4.22	The SP shall implement process and data integrity mechanisms to generate record counts to validate the completeness of data processed.	As discussed throughout this document, the SP has designed process and data integrity mechanisms to generate (for outbound files) and validate (for inbound files) the completeness of data processed.
OM 4.23	The SP shall implement process and data integrity mechanisms such that rejected data is automatically written to a suspense file and a record count made.	The SP has also designed process and data integrity mechanisms so that rejected data is automatically written to a suspense file and a record count made.
OM 4.36	The SP shall destruct confidential information, envelopes, other paper media, and electronic media in accordance with State policy (CDL CO 001-1, CDL CO 001-2).	The SP is committed to properly disposing of confidential electronic data and media in accordance with State policy (CDL CO 001-1, CDL CO 001-2)
OM 4.38	The SP shall implement a security response mechanism that provides automatic responses to security threats, including misuse of internal network resources and external network attacks. Responses may include alarms and termination of connection.	The SP is committed to implementing security response mechanisms, such as intrusion detection systems, that provide automatic responses to security threats, including misuse of internal network resources and external network attacks. Responses will include alarms and termination of connection.
OM 4.39	The SP shall implement automated virus detection on incoming and outgoing data and shall maintain current virus definitions.	All SP servers and workstations utilize McAfee® VirusScan® Enterprise 8.0.0 to automatically detect viruses on all incoming and outgoing data. We also utilize automatic updates for ensuring that virus definitions are kept current.
OM 4.40	The SP shall encrypt data that is transmitted outside the SDU facility, excluding data transmitted over the HHSDC WAN.	As discussed earlier in this document, all data transmitted outside the SDU facility, excluding data transmitted over the HHSDC WAN is encrypted. Using either F-Secure SSH® or

Req #	Detail	SP Fulfillment
		IPSec.

Table 15-1 SOW Security Requirements in Relation to Interface Testing

In addition to the SOW requirements above, we also offer the following security statements:

- The testing of all interface files will be accomplished with systems located in secure data centers operated and managed by the SP.
- All SP employees who will have access to CCSAS Production Data must read the Data Security Reminders and complete the California Confidentiality and Disclosure form provided by the State.

15.2 DATA TRANSMISSION SECURITY PROCEDURES

As discussed in section 6.5.3 – File Transfer Protocol (FTP) with interface partners, we will be utilizing F-Secure SSH® as the file exchange mechanism with our CCSAS data exchange partners. In addition, the SP will be providing the F-Secure SSH® server and client software to our CCSAS data exchange partners for the Interface Testing phase of this project.

The decision to leverage F-Secure SSH® as the file exchange mechanism was decided during the week of March 14, 2005. Given the late date of this decision, the official F-Secure Data Transmission Security procedures will be delivered prior to the Interface Test Readiness Review which is schedule for April 4, 2005. The SP plans to implement the F-Secure SSH® infrastructure during the week of March 28, 2005, and will provide installation and use procedures upon delivery to each CCSAS data exchange partner.

As discussed in section 6.5.3 - File Transfer Protocol (FTP) with interface partners, if unforeseen difficulties arise during the F-Secure SSH® implementation, we will utilize the interim procedures for using WinZip encrypting, password protecting and e-mailing the Interface Test files.

APPENDIX A: TEST SCENARIO DESCRIPTIONS

The following table shows the interface subsystem, function, test scenario, and test scenario description for the interface testing. The deferred interface test function, scenarios, and scenario descriptions are not included in this list. This provides the details of the testing that will be performed:

Subsystem	Function	Test Scenario	Test Scenario Description
Collections Engine (CE)	Start of Day	Participant Match File	Import multiple sample Participant Match Files from the BP. Validate the format, file layout and the import of the file. Validate the database updates by checking for the record counts.
Collections Engine (CE)	Start of Day	Refuse Check Instructions	Import multiple sample Refuse Check Instructions files from the State. Validate the format, file layout, and import of the file. The derogatory file is updated based on the Refuse Check Instructions file. Verify that the derogatory file has been correctly updated. Validate the database updates by checking for the record counts
Collections Engine (CE)	Intraday/Aged Exception Processing	Suspense Notification	Import multiple sample Suspense Notification files from the State. Validate the format and file layout and import of the file. Validate the database updates by checking for the record counts.
Collections Engine (CE)	Intraday/Aged Exception Processing	Suspense Update	Create and export sample Suspense Update Files to the State containing the Suspense Instructions from the Collection Engine. Validate the format; file layout and export of the file. Validate the record counts by checking against the database.

Subsystem	Function	Test Scenario	Test Scenario Description
Collections Engine (CE)	Extracts	Received Collections	Generate sample Received Collection files. Verify the file format is correct and validate the record count and database record count for the Collection Payment records. Export the Received Collections file and confirm input into the outbound destination folder.
Collections Engine (CE)	Extracts	Returned Collections	Generate sample Returned Collections extract files. Verify the file format is correct and validate the record count and database record count for the Payment records. Export the Returned Collections Extract file and confirm input into the outbound destination folder.
Collections Engine (CE)	Extracts	FMS Negative Adjustment	Generate sample FMS Negative Adjustments extract files. Verify the file format is correct and validate the record count and database record count for the FMS Negative Adjustments records. Export the FMS Negative Adjustments Extract file and confirm input into the outbound destination folder.
Disbursements Engine (DE)	Import Disbursement Instructions	SWS Disbursement Instructions	Create and import a sample SWS Disbursement Instructions file in ASCII format that includes disbursement instructions. Validate the file format and verify that the data is imported into the respective disbursement database tables. Compare the stored information with the original records.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Disbursement Response	SWS Disbursement Rejects	Validate the SWS Disbursement Instructions where required fields are missing or does not pass validation rules for a valid disbursement record import. Export the SWS Disbursement Rejects file. Validate file format.
Disbursements Engine (DE)	Disbursement Response	SWS Disbursement Delete	Create a delete request through the Disbursement web interface. Export the SWS Disbursement Delete file. Validate that the file is in XML format and includes delete confirmation information. Validate the file format, and compare the information in the SWS Disbursement Delete file with the disbursement record has a deleted status in the database.
Disbursements Engine (DE)	Disbursement Response	SWS Disbursement Origination	Export a sample SWS Disbursement Origination file in XML format that includes origination confirmation information. Validate the file format, and compare the information in the SWS Disbursement Origination file with the records in the SWS Disbursement Instructions file.
Disbursements Engine (DE)	Disbursement Response	SWS Disbursement Status	Create and export a sample SWS Disbursement Status file in XML that includes status information (for example, Notification of Change and returns). Validate the file format and compare the data in the file with the records in the disbursement database.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Disbursement Response	SWS Notification of Change	Receive Electronic Disbursement Return/NOC from the bank where records are marked for NOC. Export the SWS Notification of Change file. Validate the file format of the SWS Disbursement Notification of Change (NOC).
Disbursements Engine (DE)	Import Disbursement Instructions	ARS Disbursement Instructions	Create and import a sample ARS Disbursement Instructions file in ASCII format that includes disbursement instructions. Validate the file format and verify that the data is imported into the respective disbursement database tables. Compare the stored information with the original records.
Disbursements Engine (DE)	Disbursement Response	ARS Disbursement Rejects	Validate the ARS Disbursement Instructions where required fields are missing or does not pass validation rules for a valid import. Export the ARS Disbursement Rejects file. Validate file format.
Disbursements Engine (DE)	Disbursement Response	ARS Disbursement Delete	Create a delete request through the Disbursement web interface. Export a sample ARS Disbursement Delete file in ASCII format that includes delete confirmation information. Validate the file format. Compare the information in the ARS Disbursement Delete file with the disbursement records that have a deleted status.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Disbursement Response	ARS Disbursement Origination	Export a sample ARS Disbursement Origination file in ASCII format that includes origination confirmation information. Validate the file format. Compare the information in the ARS Disbursement Origination file with the records in the ARS Disbursement Instructions file.
Disbursements Engine (DE)	Disbursement Response	ARS Disbursement Status	Create and export a sample ARS Disbursement Status file in ASCII that includes status information (for example, returns and NOC). Validate the file format and compare the data in the file with the records in the disbursement database.
Disbursements Engine (DE)	Import Disbursement Instructions	CASES Disbursement Instructions	Create and import a sample CASES Disbursement Instructions file in EBCDIC format. Validate the file format and verify that the data is imported into the respective disbursement database tables. Compare the stored information with the original records.
Disbursements Engine (DE)	Disbursement Response	CASES Disbursement Rejects	Validate the CASES Disbursement Instructions where required fields are missing or does not pass validation rules for a valid import. Export the CASES Disbursement Rejects file. Validate file format.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Disbursement Response	CASES Disbursement Delete	Create a delete request through the Disbursement web interface. Export a sample CASES Disbursement Delete file in EBCDIC format that includes delete confirmation information. Validate the file format. Compare the information in the CASES Disbursement Delete file to validate the disbursement record has a deleted status in the database.
Disbursements Engine (DE)	Disbursement Response	CASES Disbursement Origination	Export a sample CASES Disbursement Origination file in EBCDIC format that includes origination confirmation information. Validate the file format. Compare the information in the CASES Disbursement Origination with the records in the CASES Disbursement Instructions file.
Disbursements Engine (DE)	Disbursement Response	CASES Disbursement Status	Create and export a sample CASES Response file in EBCDIC that includes status information (for example, NOC and Returns). Validate the file format and compare the data in the file with the records in the disbursement database.
Collections Engine (CE)	IDB	Standard Intercept Exchange	Import the sample Intercept Files FTB Intercept File (i.e. Lottery), EDD Intercept File from EDD, FMS Intercept File from FMS/IRS. Validate the format and layout of the files received. Validate the database updates by checking for the record counts and dollar amounts.

Subsystem	Function	Test Scenario	Test Scenario Description
Collections Engine (CE)	IDB/CSR	CSR Collections	Import multiple sample CSR Collections Files from the State. Validate the format and file layout. Validate the database updates by checking for the record counts.
Collections Engine (CE)	EFT Collections	Daily ACH Credit Collections	Import multiple sample EFT Collections data files. Validate the EFT payments for conformance with the requirements defined by NACHA for child support payments. Verify the total record count. Confirm total amount by NCP, Employer and Other State for accuracy and archive the processed file.
Disbursements Engine (DE)	Bank Interface	Positive Pay Check Issue	Create and export a sample Positive Pay Check Issue file (3300-C) that includes check information. Validate the file format. Compare the information in the Positive Pay Check Issue file with the SWS/ARS/CASES Disbursement Instructions records that contain positive payments.
Disbursements Engine (DE)	Bank Interface	Paid Check Confirmation	Create and import a sample Paid Check Confirmation file (5000-P) that includes confirmation of the checks paid. Validate the file format. Compare the stored status information with the original records to validate the status modified from Outstanding to Paid.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Bank Interface	Stop Payment Request	Create a stop payment through the Disbursement web interface. Create and export the Stop Payment Request file (4300-S). Validate the Stop Payment Request file contains the stopped payments requested through the Disbursement web interface. Validate file format.
Disbursements Engine (DE)	Bank Interface	Stop Payment Request Confirmation	Create and import a sample Stop Payment Request Confirmation file (5000-S) that contain confirmation from Bank of America of receipt of each record transmitted in the Stop Payment Request file. Validate the file format. Validate the status modified from Outstanding to Stop.
Disbursements Engine (DE)	Bank Interface	Void Payment Request	Create a void payment through the Disbursement web interface. Create and export the Void Payment Request file (4300-V). Validate the Void Payment Request file contains the voided payments requested through the Disbursement web interface. Validate file format.
Disbursements Engine (DE)	Bank Interface	Electronic Disbursement Originations (PPD)	Create and export a sample Electronic Disbursement Originations (PPD) file 3000-E that includes payments to be disbursed through direct deposit. Validate the file format and compare the records with the database for the ACH flag contains PPD.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Bank Interface	Electronic Disbursement Originations (CCD+)	Create and export a sample Electronic Disbursement Originations (CCD+) file 3000-E that includes payments to be disbursed through the electronic payment method of CCD+ transmitted to the Bank of America. Validate the file format and compare the records with the database for the ACH flag contains CCD+.
Disbursements Engine (DE)	Bank Interface	Electronic Disbursement Originations (CTX)	Create and export a sample Electronic Disbursement Originations (CTX) file 3000-E that includes payments to be fulfilled through the electronic payment method of CTX (Corporate Trade Exchange) transmitted to the Bank of America.. Validate the file format and compare the records with the database for the ACH flag contains CTX.
Disbursements Engine (DE)	Bank Interface	Electronic Disbursement Returns/NOC	Create and import a sample Electronic Disbursement Returns/NOC file. Insert the data in to the respective disbursement tables and compare the stored information with the original records to validate the disbursement record has returns and Notification of Change (NOC).
Disbursements Engine (DE)	Image Exchange	Image Archive	Import the Image Archive file from the Bank of America loaded into the IPS database. Validate the import by accessing the Disbursement web interface to view the images.

Subsystem	Function	Test Scenario	Test Scenario Description
Disbursements Engine (DE)	Check Printing	Check Disbursement Origination	Create and export a sample Disbursement Check Origination file (3000-C) that includes check printing instructions. Validate the file format. Compare the information in the file with respective disbursement tables contains to validate the disbursement record in the file has a print check instruction.
Disbursements Engine (DE)	Check Printing	Check Disbursement Confirmation	Create and export a sample Disbursement Check Confirmation file (3200-C) that includes receipts of each 3000-C file. Validate the file format. Compare the information in the file with the Check Disbursement Origination file.
SDU IVR	Disbursement History	Disbursement History	Create and export a sample Disbursement History file. Validate the file format. Import the Disbursement History file to the SDU IVR subsystem.

Table A-1 Test Scenario Descriptions

APPENDIX B: TEST SCHEDULE

The table below contains the detailed test execution calendar for the various Interface files exchanged between SDU and the Interface partners. This calendar is a work in progress and will be updated on a regular basis. Updated schedules will be communicated with the State and Interface Partners.

APRIL

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
4/1/05	SWS	Participant Match File Receive Final File From State			This will not go through CORE	
4/5/05	SWS	Print Notice Receive First File From State			SP understand this interface is not ready at this time (NR); the dates will be changed following the finalization of the requirements	
4/5/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Receive First File From IDB				
4/5/05	BOA (mock)	Daily ACH Credit Collections Test 1				
4/6/05	SWS	Print Notice Test 1			SP understand this interface is not ready at this time (NR)	
4/6/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery)				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		Test 1				
4/7/05	SWS	Enrollment/Activation/Termination Reject (ACH) Receive First File From State				
4/7/05	SWS	Enrollment/Activation/Termination Request (ACH) Receive First File From State				
4/8/05	SWS	Enrollment/Activation/Termination Reject (ACH) Test 1				
4/8/05	SWS	Enrollment/Activation/Termination Request (ACH) Test 1				
4/11/05	SWS	Participant Match File Test 1			This interface test and all remaining Participant Match File tests will be run through CIE	
4/11/05	SWS	SWS Disbursement Instructions Receive First File From State				
4/11/05	ARS	ARS Disbursement Instructions (All Types) Receive First File From State				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
4/11/05	CASES	CASES Disbursement Instructions Receive First File From State				
4/11/05	BOA (mock)	Paid Check Confirmation Test 1				
4/11/05	BOA (mock)	Stop Payment Request Confirmation Test 1				
4/11/05	BOA	Electronic Disbursement Origination CTX Test 1				
4/12/05	SWS	SWS Disbursement Instructions Test 1				
4/12/05	ARS	ARS Disbursement Instructions (All Types) Test 1				
4/12/05	CASES	CASES Disbursement Instructions Test 1				
4/15/05	BOA (mock)	Daily ACH Credit Collections Review Results Test 1				
4/18/05	SWS	Participant Match File Review Results Test 1				
4/18/05	SWS	Print Notice Review Results Test 1			SP understand this interface is not ready at this time (NR)	

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
4/18/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Review Results Test 1				
4/19/05	SWS	Enrollment/Activation/Termination Reject (ACH) Review Results Test 1				
4/19/05	SWS	Enrollment/Activation/Termination Request (ACH) Review Results Test 1				
4/19/05	SWS	Refuse Check Instruction Test 1				
4/20/05	ARS	ARS Disbursement Instructions (All Types) Review Results Test 1				
4/20/05	CASES	CASES Disbursement Instructions Review Results Test 1				
4/21/05	BOA (mock)	Paid Check Confirmation Review Results Test 1				
4/21/05	BOA (mock)	Stop Payment Request Confirmation Review Results Test 1				
4/21/05	BOA	Electronic Disbursement Origination CTX Review				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		Results Test 1				
4/22/05	BOA (mock)	Daily ACH Credit Collections Test 2				
4/25/05	SWS	Participant Match File Test 2				
4/25/05	SWS	Print Notice Test 2			SP understand this interface is not ready at this time (NR)	
4/25/05	CASES	CASES Disbursement Instructions Test 2				
4/25/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Test 2				
4/26/05	SWS	Enrollment/Activation/Termination Reject (ACH) Test 2				
4/26/05	SWS	Enrollment/Activation/Termination Request (ACH) Test 2				
4/26/05	SWS	SWS Disbursement Instructions Review Results Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
4/26/05	ARS	ARS Disbursement Instructions (All Types) Test 2				
4/28/05	BOA (mock)	Paid Check Confirmation Test 2				
4/28/05	BOA (mock)	Stop Payment Request Confirmation Test 2				
4/28/05	BOA	Electronic Disbursement Origination CTX Test 2				
4/29/05	SWS	Preliminary Receive Collections File (Minus Suspense Data) Test 1			Out bound collections file from SDU to SWS	
4/29/05	CSR	CSR Collections Receive First File From CSR				
4/29/05	BOA	Electronic Disbursement Origination, PPD Test 1				
4/29/05	BOA	Electronic Disbursement Origination, CCD+ Test 1				
4/29/05	BOA	Stop Payment Request Test 1				
4/29/05	BOA	Positive Pay Check Issues Test 1				
4/29/05	BOA	Void Payment Request Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
4/29/05	BOA (mock)	Electronic Disbursement Returns/NOC Test 1				
4/29/05	BOA (mock)	Image Archive Test 1				
4/29/05	IVR	Disbursements History Test 1				
4/30/05	Print Facility	Check Disbursement Origination Test 1				
4/30/05	Print Facility	Check Disbursement Confirmation Test 1				

Table B-1 April Test Schedule

MAY

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/2/05	SWS	Refuse Check Instruction Review Results Test 1				
5/2/05	SWS	Preliminary Suspense Notification (CSE Generated Suspense Only) Receive First File From State				
5/2/05	CSR	CSR Collections Test 1				
5/3/05	SWS	SWS Disbursement Instructions Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/3/05	SWS	SWS Disbursement Origination Test 1				
5/3/05	SWS	SWS Disbursement Status Test 1				
5/3/05	SWS	SWS Notification of Change Test 1				
5/3/05	SWS	SWS Disbursement Delete				
5/3/05	SWS	SWS Disbursement Reject Test 1				
5/3/05	CASES	CASES Disbursement Instructions Review Results Test 2				
5/4/05	ARS	ARS Disbursement Instructions (All Types) Review Results Test 2				
5/4/05	ARS	ARS Disbursement Origination Test 1				
5/4/05	ARS	ARS Disbursement Status Test 1				
5/4/05	ARS	ARS Disbursement Delete Test 1				
5/4/05	ARS	ARS Disbursement Reject Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/4/05	BOA (mock)	Daily ACH Credit Collections Review Results Test 2				
5/5/05	SWS	Participant Match File Review Results Test 2				
5/5/05	SWS	Print Notice Review Results Test 2			SP understand this interface is not ready at this time (NR)	
5/5/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Review Results Test 2				
5/6/05	SWS	Enrollment/Activation/Termination Reject (ACH) Review Results Test 2				
5/6/05	SWS	Enrollment/Activation/Termination Request (ACH) Review Results Test 2				
5/6/05	SWS	Preliminary Receive Collections File (Minus Suspense Data) Review Results Test 1			Results returned from SWS	
5/6/05	CASES	CASES Disbursement Instructions Test 3				
5/6/05	CASES	CASES Disbursement Origination Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/6/05	CASES	CASES Disbursement Status Test 1				
5/6/05	CASES	CASES Disbursement Delete Test 1				
5/6/05	CASES	CASES Disbursement Reject Test 1				
5/6/05	BOA	Electronic Disbursement Origination, PPD Review Results Test 1				
5/6/05	BOA	Electronic Disbursement Origination, CCD+ Review Results Test 1				
5/6/05	BOA	Stop Payment Request Review Results Test 1				
5/6/05	BOA	Positive Pay Check Issues Review Results Test 1				
5/6/05	BOA	Void Payment Request Review Results				
5/6/05	BOA (mock)	Electronic Disbursement Returns/NOC Review Results Test 1				
5/6/05	BOA (mock)	Image Archive Review Results Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/6/05	IVR	Disbursements History Review Results Test 1				
5/7/05	Print Facility	Check Disbursement Origination Review Results Test 1				
5/7/05	Print Facility	Check Disbursement Confirmation Review Results Test 2				
5/9/05	SWS	Refuse Check Instruction Test 2				
5/9/05	CSR	CSR Collections Review Results Test 1				
5/10/05	SWS	Preliminary Suspense Notification (CSE Generated Suspense Only) Review Results Test 1				
5/10/05	ARS	ARS Disbursement Instructions (All Types) Test 3				
5/10/05	BOA (mock)	Paid Check Confirmation Review Results Test 2				
5/10/05	BOA (mock)	Stop Payment Request Confirmation Review Results Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/10/05	BOA	Electronic Disbursement Origination CTX Review Results Test 2				
5/11/05	SWS	SWS Disbursement Instructions Review Results Test 2				
5/11/05	BOA (mock)	Daily ACH Credit Collections Test 3				
5/12/05	SWS	Participant Match File Test 3				
5/12/05	SWS	Received Collections Test 1				
5/12/05	SWS	Print Notice Test 3			SP understand this interface is not ready at this time (NR)	
5/12/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Test 3				
5/12/05	BOA	Electronic Disbursement Origination, PPD Test 2				
5/12/05	BOA	Electronic Disbursement Origination, CCD+ Test 2				
5/12/05	BOA	Stop Payment Request Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/12/05	BOA	Positive Pay Check Issues Test 2				
5/12/05	BOA	Void Payment Request Test 2				
5/12/05	BOA (mock)	Electronic Disbursement Returns/NOC Test 2				
5/12/05	BOA (mock)	Image Archive Test 2				
5/12/05	IVR	Disbursements History Test 2				
5/13/05	Print Facility	Check Disbursement Origination Test 2				
5/13/05	Print Facility	Check Disbursement Confirmation Test 2				
5/13/05	CSR	CSR Collections Test 2				
5/13/05	SWS	Enrollment/Activation/Termination Reject (ACH) Test 3				
5/13/05	SWS	Enrollment/Activation/Termination Request (ACH) Test 3				
5/16/05	SWS	SWS Disbursement Instructions Test 3				
5/17/05	SWS	SWS Disbursement				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		Origination Review ResultsTest 1				
5/17/05	SWS	SWS Disbursement Status Review Results Test 1				
5/17/05	SWS	SWS Disbursement Delete Review Results Test 1				
5/17/05	SWS	SWS Disbursement Reject Review Results Test 1				
5/17/05	ARS	ARS Disbursement Status Review Results Test 1				
5/17/05	BOA (mock)	Paid Check Confirmation Test 3				
5/17/05	BOA (mock)	Stop Payment Request Confirmation Test 3				
5/17/05	BOA	Electronic Disbursement Origination CTX Test 3				
5/18/05	ARS	ARS Disbursement Origination Review Results Test 1				
5/18/05	ARS	ARS Disbursement Delete Review Results				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		Test 1				
5/18/05	ARS	ARS Disbursement Reject Review Results Test 1				
5/18/05	CASES	CASES Disbursement Instructions Review Results Test 3				
5/19/05	SWS	Received Collections Review Results Test 1				
5/19/05	SWS	Final Suspense Notification (All Suspense) Receive First File From State				
5/19/05	CASES	CASES Disbursement Origination Review Results Test 1				
5/19/05	CASES	CASES Disbursement Status Review Results Test 1				
5/19/05	CASES	CASES Disbursement Delete Review Results Test 1				
5/19/05	CASES	CASES Disbursement Reject Review Results Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/19/05	BOA	Electronic Disbursement Origination, PPD Review Results Test 2				
5/19/05	BOA	Electronic Disbursement Origination, CCD+ Review Results Test 2				
5/19/05	BOA	Stop Payment Request Review Results Test 2				
5/19/05	BOA	Positive Pay Check Issues Review Results Test 2				
5/19/05	BOA	Void Payment Request Review Results Test 2				
5/19/05	BOA (mock)	Electronic Disbursement Returns/NOC Review Results Test 2				
5/19/05	BOA (mock)	Image Archive Review Results Test 2				
5/19/05	IVR	Disbursements History Review Results Test 2				
5/20/05	Print Facility	Check Disbursement Origination Review Results Test 2				
5/20/05	Print Facility	Check Disbursement Confirmation Review				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		Results Test 2				
5/20/05	SWS	Returned Collections Test 1				
5/20/05	SWS	Refuse Check Instruction Review Results Test 2				
5/20/05	SWS	Final Suspense Notification (All Suspense) Test 1				
5/20/05	ARS	ARS Disbursement Instructions (All Types) Review Results Test 3				
5/20/05	CSR	CSR Collections Review Results Test 2				
5/23/05	BOA (mock)	Daily ACH Credit Collections Review Results Test 3				
5/23/05	SWS	SWS Notification Of Change Test 2				
5/24/05	SWS	Participant Match File Review Results Test 3				
5/24/05	SWS	SWS Disbursement Delete Test 2				
5/24/05	SWS	SWS Disbursement Reject Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/24/05	SWS	Print Notice Review Results Test 3			SP understand this interface is not ready at this time (NR)	
5/24/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Review Results Test 3				
5/25/05	SWS	Received Collections Test 2				
5/25/05	SWS	SWS Disbursement Origination Test 2				
5/25/05	SWS	SWS Disbursement Status Test 2				
5/25/05	SWS	SWS Disbursement Delete Test 2				
5/25/05	SWS	SWS Disbursement Reject Test 2				
5/25/05	ARS	ARS Disbursement Status Test 2				
5/25/05	CASES	CASES Disbursement Instructions Test 4				
5/25/05	BOA	Electronic Disbursement Origination, PPD Test 3				
5/25/05	BOA	Electronic Disbursement Origination, CCD+ Test 3				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/25/05	BOA	Stop Payment Request Test 3				
5/25/05	BOA	Positive Pay Check Issues Test 3				
5/25/05	BOA	Void Payment Request Test 3				
5/25/05	BOA (mock)	Electronic Disbursement Returns/NOC Test 3				
5/25/05	BOA (mock)	Image Archive Test 3				
5/25/05	IVR	Disbursements History Test 3				
5/25/05	SWS	Enrollment/Activation/Termination Reject (ACH) Review Results Test 3				
5/25/05	SWS	Enrollment/Activation/Termination Request (ACH) Review Results Test 3				
5/26/05	Print Facility	Check Disbursement Origination Test 3				
5/26/05	Print Facility	Check Disbursement Confirmation Test 3				
5/26/05	SWS	SWS Disbursement Instructions Review				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
		ResultsTest 3				
5/26/05	ARS	ARS Disbursement Origination Test 2				
5/26/05	ARS	ARS Disbursement Delete Test 2				
5/26/05	ARS	ARS Disbursement Reject Test 2				
5/26/05	CSR	CSR Collections Test 3				
5/27/05	SWS	Returned Collections Review Results Test 1				
5/27/05	SWS	FMS Negative Adjustments Receive First File From State				
5/27/05	ARS	ARS Disbursement Instructions (All Types) Test 4				
5/27/05	CASES	CASES Disbursement Origination Test 2				
5/27/05	CASES	CASES Disbursement Status Test 2				
5/27/05	CASES	CASES Disbursement Delete Test 2				
5/27/05	CASES	CASES Disbursement Reject Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
5/27/05	BOA (mock)	Paid Check Confirmation Review Results Test 3				
5/27/05	BOA (mock)	Stop Payment Request Confirmation Review Results Test 3				
5/27/05	BOA	Electronic Disbursement Origination CTX Review Results Test 3				
5/31/05	SWS	FMS Negative Adjustments Test 1				
5/31/05	SWS	Final Suspense Notification (All Suspense) Review Results Test 1				
5/31/05	SWS	Print Notice Test 4			SP understand this interface is not ready at this time (NR)	
5/31/05	BOA (mock)	Daily ACH Credit Collections Test 4				

Table B-2 May Test Schedule

JUNE

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/1/05	SWS	Participant Match File Test 4				
6/1/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Test 4				
6/2/05	SWS	Final Received Collections File (All Functionality) Review Results Test 2				
6/2/05	BOA	Electronic Disbursement Origination, PPD Review Results Test 3				
6/2/05	BOA	Electronic Disbursement Origination, CCD+ Review Results Test 3				
6/2/05	BOA	Stop Payment Request Review Results Test 3				
6/2/05	BOA	Positive Pay Check Issues Review Results Test 3				
6/2/05	BOA	Void Payment Request Review Results Test 3				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/2/05	BOA (mock)	Electronic Disbursement Returns/NOC Review Results Test 3				
6/2/05	BOA (mock)	Image Archive Review Results Test 3				
6/2/05	IVR	Disbursements History Review Results Test 3				
6/2/05	SWS	Enrollment/Activation/Termination Reject (ACH) Test 4				
6/2/05	SWS	Enrollment/Activation/Termination Request (ACH) Test 4				
6/3/05	SWS	Returned Collections Test 2				
6/3/05	SWS	SWS Disbursement Instructions Test 4				
6/3/05	CASES	CASES Disbursement Instructions Review Results Test 4				
6/3/05	CSR	CSR Collections Review Results Test 3				
6/6/05	SWS	Suspense Update Test 1				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/6/05	BOA (mock)	Paid Check Confirmation Test 4				
6/6/05	BOA (mock)	Stop Payment Request Confirmation Test 4				
6/6/05	BOA	Electronic Disbursement Origination CTX Test 4				
6/7/05	ARS	ARS Disbursement Instructions (All Types) Review Results Test 4				
6/7/05	CSR	CSR Collections Test 4				
6/7/05	SWS	SWS Notification Of Change Review Results Test 2				
6/8/05	SWS	Final Received Collections File (All Functionality) Test 3				
6/8/05	SWS	SWS Disbursement Delete Review Results Test 2				
6/8/05	SWS	SWS Disbursement Reject Review Results Test 2				
6/8/05	ARS	ARS Disbursement Status Review Results Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/8/05	BOA	Electronic Disbursement Origination, PPD Test 4				
6/8/05	BOA	Electronic Disbursement Origination, CCD+ Test 4				
6/8/05	BOA	Stop Payment Request Test 4				
6/8/05	BOA	Positive Pay Check Issues Test 4				
6/8/05	BOA	Void Payment Request Test 4				
6/8/05	BOA (mock)	Electronic Disbursement Returns/NOC Test 4				
6/8/05	BOA (mock)	Image Archive Test 4				
6/8/05	IVR	Disbursements History Test 4				
6/9/05	SWS	SWS Disbursement Origination Review Results Test 2				
6/9/05	SWS	SWS Disbursement Status Review Results Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/9/05	ARS	ARS Disbursement Delete Review Results Test 2				
6/9/05	ARS	ARS Disbursement Reject Review Results Test 2				
6/10/05	SWS	Participant Match File Review Results Test 4				
6/10/05	SWS	Returned Collections Review Results Test 2				
6/10/05	SWS	FMS Negative Adjustments Review Results Test 1				
6/10/05	SWS	Print Notice Review Results Test 4			SP understand this interface is not ready at this time (NR)	
6/10/05	ARS	ARS Disbursement Origination Review Results Test 2				
6/10/05	CASES	CASES Disbursement Origination Review Results Test 2				
6/10/05	CASES	CASES Disbursement Status Review Results Test 2				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/10/05	CASES	CASES Disbursement Delete Review Results Test 2				
6/10/05	CASES	CASES Disbursement Reject Review Results Test 2				
6/10/05	IDB	Standard Intercept Exchange (FMS,EDD,FTB,Lottery) Review Results Test 4				
6/10/05	BOA (mock)	Daily ACH Credit Collections Review Results Test 4				
6/10/05	SWS	Enrollment/Activation/Termination Reject (ACH) Review Results Test 4				
6/10/05	SWS	Enrollment/Activation/Termination Request (ACH) Review Results Test 4				
6/13/05	SWS	Suspense Update Review Results Test 1				
6/13/05	SWS	SWS Disbursement Instructions Review Results Test 4				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/14/05	CSR	CSR Collections Review Results Test 4				
6/14/05	BOA (mock)	Paid Check Confirmation Review Results Test 4				
6/14/05	BOA (mock)	Stop Payment Request Confirmation Review Results Test 4				
6/14/05	BOA	Electronic Disbursement Origination CTX Review Results Test 4				
6/15/05	SWS	Final Received Collections File (All Functionality) Review Results Test 3				
6/15/05	BOA	Electronic Disbursement Origination, PPD Review Results Test 4				
6/15/05	BOA	Electronic Disbursement Origination, CCD+ Review Results Test 4				
6/15/05	BOA	Stop Payment Request Review Results Test 4				
6/15/05	BOA	Positive Pay Check Issues Review Results Test 4				

Calendar Date	Interface Partner	File Name	Receipt Date	Test Script #	Comments	Pass/ Fail
6/15/05	BOA	Void Payment Request Review Results Test 4				
6/15/05	BOA (mock)	Electronic Disbursement Returns/NOC Review Results Test 4				
6/15/05	BOA (mock)	Image Archive Review Results Test 4				
6/15/05	IVR	Disbursements History Review Results Test 4				

Table B-3 June Test Schedule

APPENDIX C: CSE PASSWORD POLICY

OVERVIEW

Security staff for DCSS, FTB and the eBHC discovered an inconsistency in the password policies for each entity. This draft policy is the standard and guidelines to be followed by the eBHC until a formal DCSS CCSAS password policy is developed.

PURPOSE

The purpose of this policy is to standardize procedures for the creation and maintenance of passwords for users accessing production CSE data.

POLICY

- Passwords must contain at least eight characters with at least three of the four attributes:
  - Uppercase alpha characters
  - Lowercase alpha characters
  - Numeric characters
  - Special characters (&,*,%, etc.)

- Passwords must be changed at least every forty-five (45) days
- After a password is reset, it must be changed by the user at the first logon attempt following the reset.
- Six iterations of a password must be used before a password can be reused.
- Passwords must contain at least 1 alphabetic & 1 non-alphabetic character.
- Passwords cannot contain the user's id, name, or nicknames.
- Passwords cannot contain restricted word or word prefixes, i.e., company name, dictionary word, computer terms and names, etc.
- A password must be used for seven consecutive days before it can be changed. The only exception to this is if a password is compromised in which case the user would have to contact the appropriate Help Desk to have the password reset, e.g. DCSS Help Desk, FTB Help Desk, etc.
- User passwords must be encrypted, if possible, when stored in files or databases on CSE systems and servers. If passwords cannot be encrypted, access to the file or database element containing the passwords must be restricted to only authorized system security administrators.
- After three unsuccessful logon attempts, the user ID must be disabled. Access would be restored by contacting the Help Desk and having the user ID reset.
- Default passwords must be changed at the first logon attempt.

ENFORCEMENT

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX D: F-SECURE SSH DATA SHEET

MAXIMIZING SECURITY FOR CRITICAL SERVERS, DATA TRANSFERS, AND CORPORATE APPLICATIONS

F-Secure® SSH is a cryptographic solution built to protect critical servers, data transfers, and corporate applications from Internet spies, hackers, and other known security threats. With F-Secure SSH, you can:

- Enable remote administration, even over the Internet, by encrypting passwords and setting up secure tunnels between critical servers and workstations.
- Transmit data without passwords and ensure that transfers are completed, even when connections have been interrupted.
- Access any TCP/IP-based application through a secure transmission tunnel.

You can use F-Secure SSH to access all major UNIX, Linux, and Windows servers from almost any client platform. And because F-Secure SSH supports a broad range of authentication mechanisms, you can easily choose the level of protection you need.

F-Secure SSH Technology

Network administrators are scrambling to close the security gaps left open by existing connectivity tools. Increasingly, they're replacing Telnet, FTP, and rlogin with a robust protocol suite called Secure Shell (SSH). SSH uses strong encryption and authentication methods to eliminate today's greatest security threats.

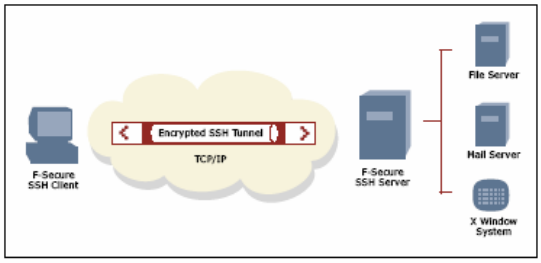
F-Secure SSH is based on the SSH protocol. It encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. F-Secure SSH has two components:

1 **An SSH client on a Windows PC or UNIX workstation**
The F-Secure SSH client includes four integrated tools:

- F-Secure SSH Terminal, which secures remote logins over unknown or untrusted networks.
- F-Secure SSH File Transfer, which safely delivers confidential data to authorized users.
- F-Secure SSH Tunnel, which creates a secure transmission link for TCP-based applications.
- F-Secure Authentication Agent, which creates and stores private keys used in the SSH public key authentication method.

2 **An SSH server on the system being accessed**
The F-Secure SSH server authenticates and encrypts traffic at the server to:

- Safeguard terminal connections.
- Forward Internet protocols, including X11, POP3, SMTP, and HTTP.
- Protect file transfers.



Together, the F-Secure SSH client and server form a secure "tunnel" through which all communications travel.

Key Features

Broad platform support
The F-Secure SSH client and server run on all major UNIX, Linux, and Windows servers—the most common corporate platforms.

IETF standard for remote administration
Standardized by the Internet Engineering Task Force, the SSH protocol is used by millions of users and thousands of organizations around the world. If you're familiar with this popular protocol, you'll find it easy to use F-Secure SSH for remote host administration.

Secure file transfers
With F-Secure SSH, you can securely copy, move, remove, and edit remote files. These operations can even be automated, scripted, and unattended to save you time.

File transfers are quick, and you can be sure that no one is eavesdropping or altering content. When interrupted, transfers will resume where they left off.

F-SECURE SSH SPECIFICATIONS

Secure tunneling of TCP traffic
F-Secure SSH lets you forward any TCP/IP traffic through an SSH connection, including POP3, SMTP, and HTTP traffic. This means you can establish encrypted connections for remote users to essential corporate applications like e-mail—without worrying about privacy protection, integrity checking, authentication, or authorization.

Certified cryptographic libraries
F-Secure SSH was the first FIPS 140-2 level 2-certified SSH solution in the world. If you work in the U.S. government, FIPS certification is a must. If you are in financial services, health care, or any enterprise where data integrity and privacy are critical, the FIPS logo ensures that you have the highest-quality cryptographic solution.

Multiple encryption algorithms and message authentication codes
F-Secure SSH provides a full spectrum of ciphers (3DES, AES 128, AES 192, AES 256, Blowfish, CAST, and DES) and message authentication codes (HMAC-MD5 and HMAC-SHA1). The options you choose will depend on your required level of interoperability, performance, and security.

Support for diverse authentication technologies
F-Secure SSH works within your established authentication infrastructure, supporting a wide range of PKI-related technologies and smart cards.

Backed by an industry-leading support organization
F-Secure SSH is distributed exclusively by WRQ, a company that is consistently rated #1 in customer support. WRQ has more than 20 years of experience dealing with remote connections to host computers. When it comes to technical support, you can expect quick, expert responses to your questions and requests.

Support
SSH Protocol 2.0: IETF SecSh Internet draft

AES, 3DES, Blowfish, Twofish, CAST128, Arcfour, and DES encryption algorithms

MD5 and SHA-1 message integrity

DSS and RSA key authentication

Diffie-Hellman key exchange method

Windows domain authentication (GSSAPI and Microsoft Kerberos)

SecurID tokens

RADIUS protocol

X509.3 certificates, CMPv2 enrollment, PKCS#12 enrollment via web browser, and CRL checking from LDAP directories

Smart card interface: PKCS#11 and MSCAPI with Microsoft system certificates

Platforms
All major UNIX versions

Microsoft® Windows® 95

Microsoft Windows 98

Microsoft Windows Me

Microsoft Windows NT

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows 2003

ABOUT WRQ

WRQ builds host-integration, terminal-emulation, and PC X-server software. We've been connecting legacy applications to emerging technologies since 1981. Our expertise helps companies get the most value from their hosts today as they advance their long-term IT strategy. Learn more about our Reflection® and Verastream® products at **www.wrq.com.**